Cybersecurity, Identity Theft, and the Limits of Tort Liability

Vincent R. Johnson

Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S. C. L. Rev. 255 (2005).

CYBERSECURITY, IDENTITY THEFT, AND THE LIMITS OF TORT LIABILITY

VINCENT R. JOHNSON*

I. THE VULNERABLE FOUNDATIONS OF MODERN SOCIETY 255

II. THE DUTY TO PROTECT DATABASE INFORMATION 263
A. *Statutes Legislatively Creating a Cause of Action* 264
B. *Statutes Judicially Determined to Set the Standard of Care* 266
1. *The Gramm-Leach-Bliley Act* 266
2. *State Security Breach Notification Laws* 270
C. *Basic Tort Principles* 272
1. Palsgraf, Kline, *and Related Cases* 272
2. *Public Policy Analysis* 276
3. *Voluntary Assumption of Duty* 278
D. *Fiduciary Obligations* 280

III. THE DUTY TO REVEAL EVIDENCE OF SECURITY BREACHES 282
A. *Statutory Duties* 283
B. *Basic Tort Principles* 288
1. *General Duty or Limited Duty* 288
2. *The Obligation to Correct Previous Statements* 291
3. *Conduct Creating a Continuing Risk of Physical Harm* 293
C. *Fiduciary Duty of Candor* 295

IV. LIMITING CYBERSECURITY TORT LIABILITY 296
A. *The Economic-Loss Rule* 296
B. *Emotional-Distress Damages* 303
C. *Security-Monitoring Damages* 305

V. CONCLUSION: SECURITY IN INSECURE TIMES 311

I. THE VULNERABLE FOUNDATIONS OF MODERN SOCIETY

In the developed world at the beginning of the twenty-first century, life is built upon computerized databases. Those electronic troves contain a vast range of

---

* Visiting Professor of Law, University of Notre Dame. Professor of Law, St. Mary's University, San Antonio, Texas. B.A., LL.D., St. Vincent College (Pa.); J.D. University of Notre Dame; LL.M., Yale University. Member, American Law Institute. Co-author, STUDIES IN AMERICAN TORT LAW (3d ed. 2005) (with Alan Gunn). Research and editorial assistance were provided by Graham D. Baker and Brenna Nava. Additional help was furnished by Claire G. Hargrove.

information about virtually all persons who interact (voluntarily or involuntarily) with the institutions of society. A myriad of entities—including businesses, non-profit organizations, and the government—assemble, update, manage, and use masses of computerized information relating to individuals.[1] The data often includes, but certainly is not limited to names, relationships (e.g., family members and employers), contact information (e.g., phone numbers, residences, and virtual addresses), personal histories (e.g., birth dates, medical data, physical characteristics, and educational records), official identifiers (e.g., social security, driver's license, and passport numbers), and financial records (e.g., bank, credit card, frequent flyer, and investment account numbers).[2] Without these databases, virtually all types of enterprises would operate much less efficiently than they do today.

When an unauthorized user hacks or otherwise improperly accesses information contained in computerized databases,[3] the consequences can be devastating for the persons to whom the information relates (data subjects). Among the more obvious risks is the possibility that an affected individual will become a victim of identity theft[4] and will suffer ruinous losses to credit and reputation,[5] emotional distress,[6]

---

1. "Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet web sites are all sources of personal information . . . ." Database Security Breach Notification Law, ch. 51, § 3072, 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw). "[B]usinesses and governments share everything from marketing lists to property records on the Internet." *CR Investigates: Stop Thieves from Stealing You*, CONSUMER REP., Oct. 2003, at 12 [hereinafter *Stop Thieves*].

2. *Identity Theft Resource Center Reports 104 Security Breaches Since January 1st; Is Anyone Hearing an Alarm Bell Yet?*, PR NEWSWIRE, Sept. 6, 2005, http://sev.prnewswire.com/computer-electronics/20050906/CLTU03406092005-1.html.

3. According to one source, "hacker" means an "[u]nauthorized user who attempts to or gains access to an information system and the data it supports." KeyBank, *Information Security Terms Glossary*, http://www.key.com/html/A-11.2.1.html (last visited Nov. 15, 2005). *See also* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 181–83 (2000) (discussing "hackers" and "crackers," the latter being hackers with criminal intent). In this Article, unless context indicates otherwise, the term "hacker" means an "outside" unauthorized user. "One of the greatest threats to the security of client computers is not the hacker, but the enemy within: trusted company employees, ex-employees, consultants, or other insiders familiar with the computer network." Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 76 (2001). The term "data intruder" as used herein encompasses both hackers and insiders without authorization to access data at the time, or for the purposes, that the person attempts to gain access.

States have passed security breach notification laws, discussed in Parts II.B.2 and III.A, to respond to the risks of harm that hackers and other intruders create. Application of these laws frequently pivots on the definition of "security breach." *See, e.g.,* CAL. CIV. CODE § 1798.82(d) (West Supp. 2005) (defining a breach of security of a database as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business"). This Article sometimes uses the terms data intrusion and security breach synonymously.

4. *See generally* R. Bradley McMahon, Note, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 627–29 (2004) (discussing how identity theft occurs); Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 MARQ. L. REV. 847, 851–52 (2005) (discussing "account

inconvenience, out-of-pocket expenses,[7] and perhaps even lost opportunities.[8] In more extreme cases, the individual to whom the information pertains may be blackmailed,[9] stalked by an assailant, or physically harmed.[10] The sources of unauthorized data access are diverse. "The perpetrators of computer intrusions may be bored juveniles, disgruntled employees, corporate spies, or organized crime networks,"[11] not to mention run-of-the-mill thieves.[12]

---

takeovers" and "true name fraud"); FED. TRADE COMM'N, NATIONAL AND STATE TRENDS IN FRAUD & IDENTITY THEFT: JANUARY-DECEMBER 2004 (2005), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf (gathering statistics); Tom Zeller, Jr., *Identity Crises*, N.Y. TIMES, Oct. 1, 2005, at C1 (stating that "[a]bout 10 million Americans fall victim each year to identity theft" and that "in about a third of those cases . . . private information is used by thieves to open new accounts, secure loans and otherwise lead parallel and often luxurious lives").

5. *See, e.g.*, White, *supra* note 4, at 847–48 (discussing a scenario wherein a husband and wife suffer a loss to their credit and reputation).

6. *See, e.g.*, Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, ¶ 12 (2003), http://law.richmond.edu/jolt/v10i1/article1.pdf (listing emotional distress as a consequence of identity theft).

7. SENATE COMM. ON CRIMINAL JUSTICE, BILL ANALYSIS, Tex. C.S.S.B. 122, 79th Leg., R.S. (2005), *available at* TX. B. An., S.B. 122, 4/7/2005 (Westlaw) (reporting that "[v]ictims spend an average of 600 hours over two to four years and $1,400 to clear their names").

8. *Be Aware and Beware of Identity Theft*, FDA CONSUMER, July-Aug. 2005, *available at* http://www.fda.gov/fdac/departs/2005/405_fda.html (stating that as a result of identity theft, "victims may lose job opportunities; may be refused loans, education, housing, or cars; or may even be arrested for crimes they didn't commit") [hereinafter FDA CONSUMER]. For example, a hacker may be able to access an admissions application, change the data submitted online, and thereby reduce the applicant's chances of being accepted. *Cf.* Robert Lemos, *USC Admissions Site Cracked Wide Open*, THE REGISTER, July 6, 2005, http://www.theregister.co.uk/2005/07/06/usc_site_cracked/print.html (discussing a flaw in a university application system that "left the personal information of users publicly accessible"); Reuters, *Colleges Struggle to Combat Identity Thieves*, BOSTON GLOBE, Aug. 21, 2005, at A19 (stating that "universities may rival financial institutions as attractive targets").

9. *See, e.g.*, Rustad, *supra* note 3, at 63 (reporting that "[a] former chemistry graduate student found a security flaw in a commercial website and demanded ransom payments to keep quiet about it").

10. *Cf.* Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003) (discussing the liability of an online investigation service that sold a victim's personal information to her killer). For a discussion of *Remsburg*, see *infra* text accompanying note 263.

11. Rustad, *supra* note 3, at 65.

12. *Cf.* Zeller, *supra* note 4, at C1 (stating that "some experts have suggested that consumers are much more likely to fall victim to a rogue employee—at a doctor's office, say, or a collection agency—than to a gang of hackers infiltrating a database").

News reports about hacking are now common.[13] Such breaches of data security often threaten the interests of hundreds or thousands of persons simultaneously.[14] Because database use is ubiquitous, virtually everyone is a potential victim.[15]

Hackers and other data intruders are subject to criminal[16] and civil liability.[17]

---

13. *See, e.g.*, John C. Ensslin, *2 CU Computers Hacked; Security Breaches Expose Personal Data on 42,900 Students, Faculty and Staff*, ROCKY MTN. NEWS, July 22, 2005, at 22A (discussing security breaches at the University of Colorado that exposed the personal data of 42,900 students, faculty, and staff members); *University to Warn of Web Security Breach*, N.Y. TIMES, July 10, 2005, at 21 (discussing plans by the University of Southern California to notify 270,000 persons that hacking occurred); Ellen Yan, *Breach of Security Personal Information of More Than 300 CUNY Law Students who Received College Loans was Online, Including Bank Information*, NEWSDAY, Sept. 27, 2005, at A03 (stating that the "Social Security numbers and other sensitive information belonging to more than 300 CUNY Law School students were accidentally posted on the Internet"); *see also* DELOITTE, 2004 GLOBAL SECURITY SURVEY 14, 22 (2004), *available at* http://www.deloitte.net/dtt/cda/doc/content/dtt_financialservices_SecuritySurvey2004_051704.pdf (reporting that a survey of major global financial institutions revealed that 83% reported a breach of computer security during the last year, and that while "outside intrusions were more common than those from the inside[], the majority of respondents have experienced both").

14. *Cf.* SENATE RULES COMM., BILL ANALYSIS, Cal. A.B. 700, 2001-2002 R.S. (2002), *available at* CA B. An., A.B. 700 Sen., 8/22/2002 (Westlaw) (reporting that "computer hackers were able to illegally access sensitive financial and personal information, including Social Security numbers, of approximately 265,000 state workers"); Eric Dash, *Europe Zips Lips; U.S. Sells ZIPS*, N.Y. TIMES, Aug. 7, 2005, § 4, at 1 (stating that, in 2005, "the personal information of more than 50 million consumers has been lost, stolen and even sold to thieves"); Eric Dash, *From Data Holders, Lots of Reassurance*, N.Y. TIMES, July 18, 2005, at C6 (indicating that Bank of America reported in February 2005 "that it had lost data tapes containing millions of its customers' records"); Melissa Sanchez, *Breach Exposes School Records*, STAR-TELEGRAM (Fort Worth, Tex.), Aug. 9, 2005 (discussing a breach of security at the University of North Texas compromised data relating to more than 38,000 present, former, and prospective students); Lemos, *supra* note 8 (discussing a flaw in an online university application system that "put at risk 'hundreds of thousands' of records containing personal information").

15. *See* David B. Reddick, *Security Breach Notification Laws: What Threats Do They Pose for Insurers?*, ISSUE BRIEF (Nat'l Ass'n of Mutual Ins. Cos., Indianapolis, Ind.), July 7, 2005, at 2 (indicating that during a recent year more than 10 million persons were victims of identity theft, which "topped the FTC's annual complaints list for the fifth year in a row"), *available at* http://www.namic.org/insbriefs/050707SecurityBreach.pdf.

16. *See* Jason Krause, *The Case of the Ethical Hacker: U.S. Request for Reversal Raises Questions About Use of Computer Fraud Law*, A.B.A. J. E-REPORT, Nov. 7, 2003 (discussing criminal liability under the federal Computer Fraud and Abuse Act); Press Release, U.S. Dep't of Justice, Federal Jury Convicts Smart-Card Hacker for Violating Digital Millennium Copyright Act (Sept. 22, 2003), http://www.usdoj.gov/criminal/cybercrime/whiteheadConviction.htm (discussing the first hacker conviction under the Digital Millennium Copyright Act); *Ex-Student Sentenced in UT Computer Hacking*, SAN ANTONIO EXPRESS-NEWS, Sept. 7, 2005, at 2B (discussing a former student sentenced to five years of probation and ordered to pay over $170,000 in restitution); *see also* CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 37–39 (Stewart D. Personick ed., 2003), *available at* http://books.nap.edu/html/ciip/index.html [hereinafter CRITICAL INFORMATION INFRASTRUCTURE] (briefly discussing the federal Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the USA Patriot Act, as well as fraud in connection with "access devices" and interception of communications); Brent Wible, *A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577, 1581–85 (2003) (discussing computer crime involving unwarranted intrusions into private computer networks). Hackers who misuse improperly accessed personal information may also be subject to liability under the identity theft laws. *See, e.g.*, White, *supra* note 4, at 856 (indicating that forty-four states have identity theft statutes and that, in 1998, Congress passed the Identity Theft and

Victims may sue, sometimes successfully,[18] under a variety of tort theories, including conversion,[19] trespass to chattels,[20] and intrusion upon private affairs,[21] as well as under the civil liability provisions of the federal Computer Fraud and Abuse Act.[22] However, hackers, particularly those located in other countries,[23] may be difficult to identify or subject to jurisdiction. Hackers may also be judgment-proof.[24] A better target for a lawsuit—one easier to locate, more amenable to legal

---

Deterrence Act).

17. *See* Rustad, *supra* note 3, at 66 (predicting that "[t]ort remedies . . . will play an increasingly important role in punishing and deterring fraud, hacking, and other wrongdoing on the Internet").

18. *See* Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 85 (2003) (stating that "[h]ardly a day goes by without new media reports of cyberspace wrongs, yet plaintiff victories remain rare"). Whether hackers have a duty to mitigate or avoid liability is a subject of debate. According to "the main principles of hacking[,] . . . information should circulate as widely as possible." Nicholas Thompson, *Who Needs Keys? Hackers Learn How to Trespass the Old-Fashioned Way—From a Lockpicker*, LEGAL AFF., Nov.–Dec. 2004, at 8, 8: *see also* Wible, *supra* note 16, at 1589–92 (discussing the transformation of hacker culture and stressing the need to "rebuild a community of hackers in which a body of positive social norms can be sustained"); Krause, *supra* note 16 (stating that "[o]ne of the activities that defines the hacker community is the process of looking for software security holes and publishing details of security flaws on the Web. . . . Some argue this research is a kind of peer review that is vital to computer science").

19. *See, e.g.*, Rustad, *supra* note 3, at 114 (opining that "a virus that destroys a hard drive might be conceptualized as the tort of conversion").

20. *See id.* at 106 (stating that "[c]ourts have held that a hacker's intrusion into a computer network constitutes a trespass to chattels").

21. *See* Shannon Duffy, *Law Firm Accused of Hacking*, LEGAL INTELLIGENCER, July 14, 2005, at 1, *available at* http://www.law.com/jsp/ltn/pubArticleLTN.jsp?id=1121245509109 (discussing a suit against a law firm for "copyright infringement, civil conspiracy, trespass to chattels, trespass for conversion, and intrusion upon seclusion").

22. 18 U.S.C. § 1030(g) (2000) (stating in part that "[a]ny person who suffers damage . . . may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief"); *see generally* Rustad, *supra* note 3, at 89–91 (describing the Computer Fraud and Abuse Act).

23. *See, e.g.*, Ensslin, *supra* note 13 (discussing attacks traced to France and Eastern Europe); Rustad, *supra* note 3, at 74 (stating that the "Russian Republics have been a popular venue for innovative cyberscams involving credit card numbers stolen from websites"); SENATE RULES COMM., BILL ANALYSIS, Cal. A.B. 700, 2001-2002 R.S. (2002), *available at* CA B. An., A.B. 700 Sen., 8/22/2002 (Westlaw) (discussing access of hacked data by "unauthorized persons in Germany").

24. *See* Wible, *supra* note 16, at 1582 (asserting that "hackers tend to be judgment proof").

process, and perhaps more solvent—may be the database possessor[25] who failed to prevent or reveal the security breach, rather than the intruder.

Whether, and to what extent, courts can hold a database possessor liable for damages suffered by data subjects as a result of improper data access are questions of huge importance. On one hand, unless the courts impose some form of liability, the persons often in the best position to prevent the losses may have insufficient incentive to exercise care to avoid unnecessary harm. On the other hand, if liability is too readily assessed, it will have the power to bankrupt valuable enterprises because of the often vast numbers of potential plaintiffs and consequent extensive resulting damages.[26] Obviously, courts must strike a balance that adequately protects the interests of individuals without discouraging the use of computer technology or driving important institutions out of existence.

---

25. There is an important initial terminological question relating to cybersecurity tort liability: if there is a duty of care and a risk of liability, on whom should the duty and risk be imposed? Should the analysis focus on the obligations of database owners, database possessors, or some other class of persons? This Article speaks in terms of the duty and liability of database "possessors" on the assumption that a party in possession of data has the opportunity to exercise care. The term would include owners or licensees in possession of data and perhaps others. The determination to focus on possession of data finds analogical support in the law of premises liability that generally imposes duties and liability on the party in possession of the premises at the time the harm occurred. For example, a lessor not in possession of a leased premises is subject to only limited liability in many states. *See, e.g.*, Clauson v. Kempffer, 477 N.W.2d 257, 261 (S.D. 1991) (holding that a landlord had no duty to warn a motorcyclist of a smooth wire fence that tenants had strung across a road on a leased premises). However, a legislature or court might elect to speak in other terms. State security breach notification statutes generally only require data owners or licensors to notify data subjects that unauthorized access to data has occurred. *See, e.g.*, CAL. CIV. CODE §§ 1798.81.5–.82 (West Supp. 2005) (imposing obligations on a "business that owns or licenses personal information"); Act effective July 1, 2005, ch. 473, sec. 1, §§ 47-18-2107(a)(2), -2107(b), 2005-2 Tenn. Code Ann. Adv. Legis. Serv. 749, 749-50 (LexisNexis) (imposing a notification duty on an "information holder," which includes "any person or business that conducts business in this state, or any agency of the State of Tennessee or any of its political subdivisions"). State security breach notification laws generally oblige database possessors who do not own the breached data to disclose the intrusion to the owner of the data, rather than the data subject. *See, e.g.*, CAL. CIV. CODE § 1798.82(b) (West Supp. 2005) (stating that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person").

26. *See* Robert Steinberg, *Advising Clients About Hacker Insurance*, LOS ANGELES LAW., Feb. 2003, at 60, 60 ("For corporations with well-known brand names, in high visibility industries, with significant Web presences, or sensitive information, a single breach, with the potential for third-party claims, can be financially devastating."); *see also* Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457, 491 (2004) ("One study found that publicly-traded firms which disclosed security breaches lost 2.1% of their market value within two days of the disclosure.").

Parties are now litigating cases over the liability of database possessors,[27] and lawyers are starting to advise clients about the risk that they may be accountable for harm caused by hackers and other intruders.[28] However, despite the recent enactment of security breach notification statutes in at least eighteen states,[29] the law governing database possessor liability is far from settled. Considerable uncertainty exists regarding the reach of the new state laws and related concerns, including what types of damages plaintiffs might recover in tort actions involving data intrusion. This Article addresses three key questions relating to database possessor liability for harm caused by data intruders.[30]

---

27. *See, e.g.*, Complaint at 2–3, Parke v. Cardsystems Solutions, Inc., No. CGC-05-442624 (Cal. Super. Ct. filed June 27, 2005) (alleging, in a class action, that hackers accessed information relating to forty million credit card accounts and that the defendants had failed to protect the data or promptly notify data subjects about the breach); Class Action Complaint, Goldberg v. ChoicePoint, Inc., No. BC329115 (Cal. Super. Ct. filed Feb. 18, 2005) (alleging, in a class action involving 145,000 persons, that the defendants failed to protect personal data, failed to promptly notify data subjects of the breach, engaged in unfair business practices, and committed fraud and negligent misrepresentation); *see also* Laura Mahoney, *Identity Theft: Class Action Filed Against ChoicePoint as AG Launches Investigation into Breach*, 6 COMPUTER TECH. L. REP. 107 (2005) (indicating that the state was "tracking about 45 cases that have been significant in size").

28. *See* Jane Strachan, *Cybersecurity Obligations*, 20 ME. B.J. 90 (2005) (discussing how to advise business clients in light of "[t]oday's . . . risk of a lawsuit or regulatory enforcement arising from inadequate information security practices").

29. *See* ARK. CODE ANN. §§ 4-110-101 to -108 (Supp. 2005); CAL. CIV. CODE §§ 1798.80–.84 (West Supp. 2005); GA. CODE ANN. §§ 10-1-910 to -912 (Supp. 2005); MONT. CODE ANN. § 31-3-115(5) (2005); N.D. CENT. CODE §§ 51-30-01 to -07 (Supp. 2005); Act of June 24, 2005, Pub. Act 05-148, §§ 1-3, 2005 Conn. Legis. Serv. (West), *available at* CT LEGIS P.A. 05-148 (Westlaw); Act of June 28, 2005, Pub. Act 61, sec. 1, §§ 12B-101 to -104, 2005 Del. Code Ann. Adv. Legis. Serv. (LexisNexis), *available at* 2005 Del. ALS 61 (LexisNexis); Act of June 14, 2005, ch. 2005-229, sec. 1-3, §§ 817.568-.5681, 2005 Fla. Sess. Law Serv. (West), *available at* FL LEGIS 2005-229 (Westlaw); Personal Information Protection Act, Pub. Act 94-36, ch. 815, sec. 530, 2005 Ill. Legis. Serv. (West), *available at* IL LEGIS 94-36 (2005) (Westlaw); Act effective July 1, 2005, Pub. L. No. 91-2005, ch. 11, sec. 2, §§ 4-1-11-1 to -9, 2005 Ind. Legis. Serv. (West), *available at* IN LEGIS 91-2005 (2005) (Westlaw); Database Security Breach Notification Law, ch. 51, §§ 3071 to -3077, 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw); Notice of Risk to Personal Data Act, ch. 379, sec. 1, §§ 1346 to -1349, 2005 Me. Legis. Serv. (West), *available at* ME LEGIS 379 (2005) (Westlaw); Act of June 2, 2005, ch. 167, sec. 1, §§ 1 to -6, 2005 Minn. Sess. Law Serv. (West), *available at* MN LEGIS 167 (2005) (Westlaw); Act of June 17, 2005, ch. 486, sec. 1, §§ 4 to -6, 2005 Nev. Stat., *available at* NV LEGIS 486 (Westlaw); Act of June 17, 2005, ch. 485, sec. 1, §§ 17 to -30, 2005 Nev. Stat., *available at* NV LEGIS 485 (2005) (Westlaw); Rhode Island Identity Theft Protection Act of 2005, ch. 225, sec. 1, §§ 11-49.2-1 to –.2-7, 2005 R.I. Gen. Laws Adv. Legis. Serv. (LexisNexis), *available at* 2005 R.I. ALS 225 (LexisNexis); Act effective July 1, 2005, ch. 473, sec. 1, § 47-18-2107, 2005-2 Tenn. Code Ann. Adv. Legis. Serv. 749, 749-51 (LexisNexis); Identity Theft Enforcement and Protection Act, ch. 294, sec. 2, §§ 48.001 to -.203, 2005 Tex. Sess. Law Serv. (West), *available at* TX LEGIS 294 (2005) (Westlaw); Act of May 10, 2005, ch. 368, §§ 1 to -2, 2005 Wash. Legis. Serv. (West), *available at* WA LEGIS 368 (2005) (Westlaw); *see generally* Reddick, *supra* note 15 (analyzing security breach notification laws for an insurance trade association).

30. A database possessor may "lose" the personal information of others in a variety of ways. For example, the possessor might (1) fail to protect the information from hackers and other intruders; (2) erroneously release the information to third persons; or (3) simply misplace the data. In one sense, these three forms of data loss each involve alleged failure to exercise reasonable care, and in that respect, they may be nothing more than different examples of negligent data handling. However, on closer scrutiny, the three types of data loss identified above may be legally distinguishable. Failure to guard against

The first issue, considered in Part II, is whether database possessors have a legal duty to safeguard data subjects' personal information from unauthorized access by hackers or others. The discussion addresses the obligations imposed by statutes, ordinary tort principles (including the rules on voluntary assumption of duty), and fiduciary-duty law. Part II concludes that, in a wide range of circumstances, database possessors have (or should have) a legal obligation to data subjects to exercise reasonable care in safeguarding personal data from intruders. However, as discussed below, the precise theory under which the law imposes that duty may have important implications for defining the scope of liability.

The next issue, considered in Part III, concerns not whether there is a duty *to protect* computerized information from intruders, but whether a database possessor has a legal obligation *to disclose* evidence of a security breach to data subjects once an intrusion occurs. The discussion considers statutory obligations as well as basic tort principles. The relevant legislation includes the security breach notification laws recently passed in many states.[31] Pertinent common law guidance encompasses the basic principles of negligence liability and two specific rules that warrant special attention. The first rule, under the law of misrepresentation, imposes a duty to update previously accurate statements that are the basis for pending or continuing reliance.[32] This rule is relevant because a breach of data security may cast substantial doubt on the continuing accuracy of expansive statements about data security that are often contained in business advertisements or published privacy policies. The second rule, under failure-to-act jurisprudence, creates a duty to exercise reasonable care to prevent harm or minimize adverse consequences if prior conduct, "even though not tortious," creates a "continuing risk of physical harm."[33] This rule may be relevant because the security practices of database possessors, even if not negligent, often contribute to the success of hackers and other intruders. Finally, Part III considers the heightened candor obligations imposed by fiduciary-duty law. Part III concludes that in many situations there is (or should be) a duty,

---

intruders raises the issue of whether there is a duty to undertake what amounts to crime fighting efforts, which is a point of some controversy. *See* Dupont v. Aavid Thermal Techs., Inc., 798 A.2d 587, 592 (N.H. 2002) (stating that an employer has no broad duty to protect an employee from foreseeable crimes because "the general duty to protect citizens from criminal attacks is a government function"). In contrast, the duty to protect third persons from criminal intruders is not a significant concern in cases involving erroneous release or careless loss of data. Similarly, when database owners publish the wrong data, an exercise (albeit an imprudent exercise) of First Amendment rights to free speech or free press has occurred. The constitutional principles that have evolved to constrain the imposition of tort liability for utterances resulting in defamation or incitement might arguably also limit the levying of tort liability for erroneous publication of data that causes harm. However, those same principles would have no application in suits involving hacked or misplaced data because the database possessor never had an intent to speak or publish anything in those situations. Tort literature has not yet fully explored the issues relating to these various types of data losses. This Article is primarily concerned with a database possessor's duty to protect data from intruders.

31. *See supra* note 29 and accompanying text.

32. *See, e.g.*, McGrath v. Zenith Radio Corp., 651 F.2d 458, 468 (7th Cir. 1981) (holding that the failure to correct earlier true statements which have become false or misleading was fraudulent).

33. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1, 2005) (discussing duty based on prior conduct).

enforceable in a tort action for damages, to inform data subjects that the security of their data has been compromised.

The final key issue, addressed in Part IV, concerns how far the liability of a database possessor should extend in cases where the possessor has failed to exercise reasonable care to protect data or to disclose information about intrusion. The discussion first considers the economic-loss rule[34] and concludes that the rule presents an important, but limited, obstacle to recovery of tort damages. In certain circumstances, economic damages caused by identity theft resulting from improperly accessed data should be recoverable. Part IV then addresses the issue of emotional-distress damages and considers the arguments favoring limited liability for this type of loss in cybersecurity litigation. Part IV discusses the guidance that has emerged from the courts in fear-of-disease cases and recommends adapting those principles to the context of improperly accessed data. Emotional-distress damages should be available only when an intruder actually accesses a plaintiff's data, and not when that data was merely exposed to a risk of unauthorized access. Lastly, Part IV argues that, in the absence of aggravated tortious conduct (e.g., recklessness or worse), the interests of society will be best served by limiting recoverable losses to the cost of "security-monitoring" damages once a database possessor discloses to the affected individual the fact that someone has improperly accessed his or her data. This approach will encourage database possessors to discover and reveal instances of data intrusion. It will also place data subjects in a position to protect their own interests by monitoring their economic and personal security when heightened vulnerability exists. This security-monitoring damages proposal is similar in concept to medical-monitoring damages,[35] losses that many states permit victims of toxic exposure to recover. The proposed limitation on liability will encourage the exercise of care by both database possessors and data subjects, while at the same time minimizing the risk of imposing the type of extensive tort damages that would discourage the use of computer technology or impose disproportionate liability.

II. THE DUTY TO PROTECT DATABASE INFORMATION

Tort liability depends on the existence of a legal duty to exercise care that runs from the defendant (the database possessor) to the plaintiff (the data subject). Both

---

34. *See generally* Jay M. Feinman, *Doctrinal Classification and Economic Negligence*, 33 SAN DIEGO L. REV. 137, 146 (1996) [hereinafter *Doctrinal Classification*] ("[T]he economic loss rule distinguishes purely pecuniary losses from losses due to personal injury or property damage . . . as the criterion that governs the classification of cases. Economic losses are losses due to disappointed expectations, and should therefore be governed by contract law; only losses due to personal injury or property damage, which generally are not the subject of prior bargaining and which invoke public safety concerns, are within the realm of tort law.").

35. "In the context of a toxic exposure action, a claim for medical monitoring seeks to recover the cost of future periodic medical examinations intended to facilitate early detection and treatment of disease caused by a plaintiff's exposure to toxic substances." Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 821 (Cal. 1993) (citing Ayers v. Twp. of Jackson, 525 A.2d 287, 308 (N.J. 1987)). *See also* Badillo v. American Brands, Inc., 16 P.3d 435, 439 (Nev. 2001) (noting that "a growing number of appellate courts have recognized medical monitoring (seventeen states plus the District of Columbia)").

statutes and common law may impose that duty of care. The following subparts discuss legislation bearing on the question of whether a tort duty to safeguard the security of computerized personal data exists, and how ordinary tort principles and fiduciary-duty law provide two obvious sources of common law guidance on that question.

A. Statutes Legislatively Creating a Cause of Action

A statute may impose a duty to exercise care to protect data from intruders,[36] either by the legislation's express terms[37] or by a court's holding that a statute which is silent as to civil liability sets the appropriate standard of care for a tort action.[38] This subpart discusses statutes that expressly create a civil cause of action based on lack of data security. The next subpart discusses statutes that do not create a tort cause of action, but that courts may embrace as setting the standard of care for suits involving an allegedly negligent failure to safeguard computerized personal data.

An important example of legislation expressly creating a civil cause of action for failure to protect data is California's much-discussed[39] Security Breach Information Act (SBIA).[40] The SBIA was the first law in the United States to impose on businesses a duty to inform data subjects of unauthorized intrusion into their personal data.[41] The California Act has served as a model for legislation subsequently adopted in other jurisdictions.[42] Mutual concerns animate the various state laws, which often share a common language and structure. All of the laws impose a duty to reveal information about security breaches,[43] but the statutes differ in important respects. One key difference concerns whether the statutes expressly impose a duty to protect data in addition to the notification duty. Another difference concerns whether a breach of the duties imposed by the act is expressly actionable in a private lawsuit.

---

36. *See* Rustad, *supra* note 3, at 108 ("A hospital has a statutory duty to protect the privacy of its patients' records.").

37. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 cmt. b (Proposed Final Draft No. 1, 2005) (discussing express and implied statutory causes of action).

38. Sometimes courts find an "implicit" legislative intent to create a civil cause of action; other times they simply hold that the statute is an appropriate expression of the standard of care. *See* VINCENT R. JOHNSON & ALAN GUNN, STUDIES IN AMERICAN TORT LAW 305–06 (3d ed. 2005) ("In the one case, the court is saying that the legislation sets the standard because the legislature implicitly intended it to do so, and in the other case, the court acknowledges that the statute sets the standard because the court thinks that is a good idea. Either way, if the statute does not expressly create a cause of action, the essential inquiry is the same: was the law intended to protect this class of persons from this type of harm.").

39. *See, e.g.*, Preston & Turner, *supra* note 26, at 461–63 (discussing the contours of the California SBIA).

40. Act effective July 1, 2003, ch. 915, 2002 Cal. Legis. Serv. (West), *available at* CA LEGIS 915 (2002) (Westlaw).

41. *See* Reddick, *supra* note 15, at 2.

42. *See id.* at 1 (indicating that "most new laws follow the California security breach notification SBIA").

43. For a discussion of the notification laws, see *infra* Part III.A.

The California SBIA imposes a data protection obligation and expressly authorizes maintenance of a suit for damages for breach of that duty.[44] The relevant language, which became effective July 1, 2003,[45] states, "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[46] The legislation further provides, "Any customer injured by a violation of this title may institute a civil action to recover damages."[47]

The SBIA leaves no doubt that businesses owe a legal duty to customers under California law to protect customers' personal information, and that customers may recover damages if businesses breach that duty. The civil actions that the California legislature has allowed the courts to entertain are rooted in principles of negligence (rather than, for example, strict liability or recklessness), for the law speaks of "*reasonable* security procedures and practices"[48] that are "appropriate to the nature of the information."[49] Reasonableness assessed under the circumstances is the essence of the negligence standard of care. Only *unreasonable* (i.e., negligent) conduct violates the California SBIA. However, beyond offering clear guidance regarding the existence of duty and the liability regime, the SBIA leaves many matters unsettled.[50] The Act makes no attempt to define what constitutes "reasonable security procedures and practices." Presumably, that assessment is left to the finder of fact for determination on a case-by-case basis. More importantly, the SBIA gives no indication as to what types of damages plaintiffs can recover.[51]

---

44. Act effective July 1, 2003, ch. 915, 2002 Cal. Legis. Serv. (West), *available at* CA LEGIS 915 (2002) (Westlaw).

45. *See* Daniel J. McCoy, *Recent Privacy Law Developments Affecting the Workplace*, 788 PLI/PAT 435, 489 (May 2004) (discussing the California SBIA).

46. CAL. CIV. CODE § 1798.81.5 (West Supp. 2005). The statute broadly defines the term "business." *See id.* at § 1798.80(a). However, section 1798.81.5 does not apply to certain specified entities including, among others, certain healthcare providers and financial institutions. *See id.* § 1798.81.5(e). The obligations the California statute imposes reach "well beyond California's borders, potentially affecting any company, person or agency that has a computer database containing any California resident's 'personal information.'" Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals with ID Theft: The Promise and the Problems*, BUS. L. TODAY, May-June 2004, at 37, 37. Significantly, "the law only applies when an individual's 'unencrypted data' is at issue." *Id.* at 41.

47. CAL. CIV. CODE § 1798.84(b) (West Supp. 2005).

48. *Id.* § 1798.81.5 (b) (emphasis added).

49. *Id.* § 1798.81.5(c).

50. The fact that liability arises from negligence may mean that an action is subject to a comparative negligence defense. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 cmt. b (Proposed Final Draft No. 1, 2005) (stating that in dealing with a "liability right expressly created by [a] statute[,] . . . the court may need to consider whether traditional tort defenses such as comparative negligence should be deemed impliedly incorporated into the statutory cause of action"). *But see* Seim v. Garavalia, 306 N.W.2d 806, 811–13 (Minn. 1981) (discussing situations where statutes impose absolute liability).

51. While adoption of the SBIA was pending, the Information Technology Association of America (ITAA) wrote to the state Senate Committee on Privacy, raised the "specter of lawsuits targeting companies for even innocent mistakes," and requested amendments to "cap the liability

Whether those damages include compensation for personal injury, property damage, emotional distress, economic loss, or other types of harm is left unresolved. If the legislature intended for courts to allow recovery of the usual types of damages that they award in negligence suits, the scope of damages, as discussed in Part IV, may be more limited than it first appears.

B. Statutes Judicially Determined to Set the Standard of Care

Some statutes addressing issues relating to data protection do not expressly create a civil cause of action. In this category are the federal Gramm-Leach-Bliley Act of 1999 (GLBA)[52] and certain state security breach notification laws. The following subparts discuss these various pieces of legislation.

1. The Gramm-Leach-Bliley Act

The GLBA states that "[i]t is the policy of the Congress that each financial institution has *an affirmative and continuing obligation* to respect the privacy of its customers and *to protect the security and confidentiality of those customers' nonpublic personal information.*"[53] In furtherance of that policy, the Act requires a significant number of state and federal governmental entities[54] to establish[55] and enforce[56] "appropriate standards for the financial institutions[57] subject to their jurisdiction."[58] Those standards must provide

> administrative, technical, and physical safeguards—
>
> (1) to insure the security and confidentiality of customer records and information;

---

exposure." Calif. Bill Analysis, Senate Floor, 2001–2002 Regular Session, Assembly Bill 700, Aug. 22, 2002, *available in* Westlaw at CA B. An., A.B. 700 Sen., 8/22/2002. However, the ITAA offered no suggestion for how to effectuate such a cap, and the Committee report simply notes that "AB 700 does not create any new penalty in law." *Id.*

52. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of Titles 12 and 15 of the United States Code).

53. Gramm-Leach-Bliley Act § 501(a) (codified at 15 U.S.C. § 6801(a) (2000)) (emphasis added).

54. 15 U.S.C. § 6805 (defining entities and roles); *see also* 15 U.S.C. § 6825 (stating that "each Federal banking agency . . . , the National Credit Union Administration, and the Securities and Exchange Commission or self-regulatory organizations, as appropriate, shall review regulations and guidelines applicable to financial institutions under their respective jurisdictions and shall prescribe such revisions to such regulations and guidelines as may be necessary to ensure that such financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect [the solicitation or obtaining of customer information by false pretenses]").

55. 15 U.S.C. § 6801(b) (discussing establishment of regulations).

56. 15 U.S.C. § 6805(a) (providing that the regulations "shall be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction").

57. "Financial institutions under the Act include everything from real estate appraisers to automobile dealerships." McMahon, *supra* note 4, at 634–35.

58. 15 U.S.C. § 6801(b).

> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[59]

The GLBA does not expressly create a civil cause of action against financial institutions for breach of their duty to protect customer information.[60] However, one commentator has suggested[61] that the provisions of the Act, or the standards adopted pursuant to the Act, might serve as the predicate for a tort action under a negligence per se theory.[62]

Under negligence per se, a court may, in its discretion, embrace a statute not expressly providing for a civil cause of action as the standard of care for a tort suit. If the legislature intended the enactment to protect the class of persons of which the plaintiff is a member from the type of harm that occurred, a court may determine that violation of the statute defines the appropriate terms for imposing civil liability.[63] For example, courts have frequently adopted traffic rules[64]—such as those requiring drivers to travel in the proper lane,[65] use headlights after dark,[66] or not exceed the speed limit[67]—as setting the standard of care in auto accident cases

---

59. 15 U.S.C. § 6801(b) (2000).

60. Julia C. Schiller, Comment, *Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?*, 11 COMMLAW CONSPECTUS 349, 359 (2003) ("The GLB Act . . . does not provide for a private right of action for consumers to sue the financial institution directly for violation of the statute.").

> The consumer must complain to the agency having jurisdiction over them and that agency may bring a court action against the financial institution. However, some state laws, such as the Unfair and Deceptive Practice Laws, may enable the consumer to claim that a violation of the GLB Act violated other rights granted to the individual by the state.

Id.

61. *See* White, *supra* note 4, at 865–66 (discussing negligence per se under the GLBA).

62. *See generally* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 (Proposed Final Draft No. 1, 2005) (discussing negligence per se). In most jurisdictions, the unexcused violation of a standard-setting statute is conclusive proof of breach of duty and constitutes negligence per se, *see generally id.* § 14 cmt. c, or prima facie negligence, *see, e.g.*, Mich. Dep't of Transp. v. Christensen, 581 N.W.2d 807, 809 (Mich. Ct. App. 1998). Regardless of the precise procedural effect of establishing an unexcused violation, a determination that the enactment is controlling affirms that a legal duty runs from the defendant to the plaintiff. The jury is not free to ignore that determination. *See* Martin v. Herzog, 126 N.E. 814, 815 (N.Y. 1920) (stating that "[j]urors have no dispensing power").

63. *See generally* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 (Proposed Final Draft No. 1, 2005) (discussing relevant considerations).

64. *See id.* § 14 cmt. d (noting that "in most highway-accident cases, findings of negligence depend on ascertaining which party has violated the relevant provisions of the state's motor-vehicle code").

65. *See Martin*, 126 N.E. at 814–15 (discussing negligence predicated on failure to stay to the right of the center of the highway, as required by statute).

66. *See id.* at 815 (holding that the failure of a wagon driver to display the lights required by a highway law was negligent).

67. *See* Griffith v. Schmidt, 715 P.2d 905, 911 (Idaho 1985) (holding that exceeding the speed limit was negligence per se).

because the intent of those laws is to protect others on the road from the risk of physical harm. Referring to legislative enactments in tort litigation serves the "function of simplifying or providing structure to the rendering of negligence determinations."[68] Such reference also helps ensure consistency in resolving issues of recurring importance and provides clear notice to others as to what should be done in given circumstances.

However, a court may take into account factors other than the class of persons and the type of harm in determining whether a statute silent as to civil liability appropriately defines what society expects of a reasonably prudent person. For example, a court should not embrace a statute that is obsolete,[69] vague,[70] or duplicative of existing common law obligations as the basis for civil liability.[71] Similarly, if the legislature intended the penalties for violation of a law to be minimal or limited only to those set forth in the enactment, a court should not rely on the law as a basis for imposing other legal obligations.[72]

The GLBA is an important expression of public policy that courts should take into account in determining whether database possessors, or some subset thereof (e.g., financial institutions or businesses generally), have a legal duty to protect information relating to data subjects that is enforceable in a tort action.[73] Indeed, as an enactment of Congress, the nation's highest legislative body, the language of the GLBA is entitled to great weight in resolution of the duty question. However, courts should not interpret the GLBA itself as setting the standard of care for a civil cause of action because it lacks specificity as to precise requirements of a reasonable financial institution.[74] In contrast to a law that gives clear notice of

---

68. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 cmt. e (Proposed Final Draft No. 1, 2005).

69. *See* RESTATEMENT (SECOND) OF TORTS § 286 cmt. d (1965) (discussing obsolescence).

70. *See, e.g.*, Perry v. S.N., 973 S.W.2d 301, 302, 309 (Tex. 1998) (holding that a statute imposing a reporting requirement on "any person having cause to believe [that] a child [was] being abused" was not an appropriate standard for negligence per se liability because, among other things, the statutory standard was unclear).

71. *See generally* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 cmt. e (Proposed Final Draft No. 1, 2005) (noting that negligence per se in the case of a statute duplicating the common law does nothing to aid the court in determining negligence).

72. *See id.* § 14 cmt. c ("If the statute does include . . . a provision [making the statutory violation irrelevant in a common law action for damages], courts should of course honor it . . . ."); *see also* Pool v. Ford Motor Co., 715 S.W.2d 629, 631 (Tex. 1986) (holding that the lower court misapplied two statutes, one that provided that the presumption of intoxication would not apply in civil actions, and another that stated that "maximum or minimum speed limitations shall not be construed to relieve the plaintiff in any action from the burden of proving negligence" (quoting TEX. REV. CIV. STATE. ANN. art 6701d, § 171(b) (Vernon 1977) (repealed 1995))).

73. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 46 n.29 ("It could be argued that financial institutions have an existing duty under the Gramm-Leach-Bliley implementing regulations to provide immediate and effective incident response to protect the confidentiality of consumer data maintained on their own networks").

74. *Cf.* County of Dallas v. Poston, 104 S.W.3d 719, 722–23 (Tex. App. 2003) (holding that because the statutory duty of a motor vehicle operator crossing a highway to yield the right-of-way to an approaching vehicle is not absolute, the statute was not a proper basis for a finding of contributory negligence as a matter of law; the appropriate inquiry is whether a reasonably prudent driver under the same or similar circumstances would have yielded the right-of-way).

expectations—such as a statute that requires a pedestrian to walk on the sidewalk, not in the street,[75] or to yield to all vehicles already on the road[76]—the GLBA offers no clear guidance as to exactly what a financial institution must do to avoid liability. The Act is vague and speaks of an obligation to protect data security without indicating what must be done to fulfill that obligation. The GLBA's vagueness, coupled with its failure to provide for civil liability, means that the questions of whether there is a tort duty, and, if so, what that duty requires, are issues that the courts must still resolve. Of course, "the presence of a statutory requirement that is binding on the defendant, and the court's awareness of the legislature's assumptions in imposing that requirement, can be important points for the court to consider in determining whether a duty exists."[77] But the question of duty requires judicial determination. Consequently, insofar as the GLBA is concerned, it is not useful to speak of negligence per se.[78]

The same analysis would not necessarily apply to the regulations adopted pursuant to the mandates of the GLBA. Unlike the statute itself, the provisions adopted to implement its mandates might be sufficiently specific to define what action financial institutions must take with regard to protecting data security. However, the standards agencies have already adopted, such as those issued by the Federal Trade Commission (FTC),[79] are typically flexible in nature, equivocal as to what must be done, and generally unsuited to defining the conduct expected of a reasonably prudent financial institution. The FTC standards require financial institutions subject to the Commission's jurisdiction to develop and implement a

---

75. *See, e.g.*, Zeni v. Anderson, 243 N.W.2d 270, 273 (Mich. 1976) (discussing a sidewalk statute).

76. Ranard v. O'Neil, 531 P.2d 1000, 1003 (Mont. 1975).

77. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 cmt. i (Proposed Final Draft No. 1, 2005).

78. *Cf. id.* § 14 cmt. e ("Many statutes impose obligations on actors that largely correspond to or codify obligations imposed by negligence law . . . . Thus a statute might require motorists to drive their vehicles at a 'reasonable and prudent' speed, or might prohibit driving the vehicle 'carelessly.' To find that an actor has violated such a statute, the jury would also need to find that the actor has behaved negligently. In such situations, the doctrine of negligence per se is largely superfluous in ascertaining the actor's liability. . . . [C]ourts sometimes allow parties to argue negligence per se as a supplement to ordinary negligence; but more frequently they reject negligence per se, recognizing its redundancy . . . ."); *see also* Louisiana-Pac. Corp. v. Knighten, 976 S.W.2d 674, 675 (Tex. 1998) (holding that a statute governing the responsibility of a driver following another vehicle—which required the driver to proceed safely and safely bring a vehicle to a stop—imposed a duty of reasonable care on the driver and precluded the leading driver from obtaining a negligence per se instruction in an action arising out of a rear-end collision).

79. *See* Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1–.5 (2005); *see also* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 57–58 (stating that "[o]n May 17, 2002, the FTC issued the Safeguards Rule, which implements the safeguard provisions required by the Gramm-Leach-Bliley Act. The Safeguards Rule requires covered entities to implement a comprehensive information security program by May 23, 2003, to ensure the security, confidentiality, and integrity of nonpublic customer information against both internal and external threats. Institutions that fail to comply could face potential FTC enforcement actions and potential liability under state consumer protection laws or common law claims (such as negligence)").

written security plan "appropriate"[80] to their size and complexity which takes into account various sources of risk,[81] regularly tests the effectiveness of its "safeguards' key controls, systems, and procedures,"[82] and undergoes periodic adjustment as necessary.[83] Thus, the standards simply endorse a process by which financial institutions must address security issues. Like the GLBA itself, the FTC standards offer no clear guidance as to precisely what precautions financial institutions must implement to protect data security. The same is true of the federal Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which address the obligations imposed by the GLBA.[84] As yet, no reported cases have held that the data security provisions[85] of the GLBA or related regulations, or other federal laws,[86] set the standard of care for a consumer's tort action against a financial institution.

2. State Security Breach Notification Laws

Certain state security breach notification laws that require database possessors to protect personal information from unauthorized access make no provision for

80. *See* 16 C.F.R. § 314.3(a) (stating that financial institutions "shall develop, implement, and maintain a comprehensive information security program that is written . . . and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue").

81. *See id.* § 314.4(b) ("At a minimum, . . . a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.").

82. *Id.* § 314.4(c).

83. *See id.* § 314.4(e) (requiring adjustments in light of "any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program").

84. *See* 12 C.F.R. Pt. 30, App. B (2005). One provision in the Interagency Guidelines that has some degree of specificity concerns service providers. The Guidelines state that "[e]ach bank shall . . . [r]equire its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines." *Id.* However, this rule is unlikely to serve as a helpful standard for resolving tort litigation brought by customers. The plaintiff would have to show that not only did the service provider fail to employ appropriate safeguards, but also that the failure would not have occurred except for the absence of a contractual provision. Such a finding would entail a degree of speculation by the fact-finder, and might present the type of causation problem that is sufficient to dissuade a court from embracing a rule as establishing the threshold for liability. *See* Stachniewicz v. Mar-Cam Corp., 488 P.2d 436, 438 (Or. 1971) (declining to hold that a dram shop statute set the standard of care because doing so would complicate the causation assessment).

85. The GLBA also regulates extensively the sharing of personal data between institutions. A violation of those provisions does not give an affected individual a private cause of action. *See* Menton v. Experian Corp., No. 02 Civ. 4687 (NRB), 2003 WL 21692820, at *3 (S.D.N.Y. July 21, 2003) (finding, in dicta, no private right of action).

86. *See generally* Preston & Turner, *supra* note 26, at 471–77 (discussing data security provisions in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Children's Online Privacy Protection Act (COPPA)).

civil liability.[87] Some of these laws may nevertheless leave room for judicial recognition of a civil cause of action. For example, the Arkansas Personal Information Protection Act,[88] which provides only for enforcement by the attorney general,[89] states that the Act "does not relieve a person or business from a duty to comply with any *other* requirements of *other* state and federal law regarding the protection and privacy of personal information."[90] However, the use of the word "other" seems to suggest that a court should not embrace the security breach notification law, by itself, as the basis for a civil cause of action.

Similarly, it is difficult to envision that the Texas state security breach statute could be a predicate for a negligence per se claim. The Texas law,[91] like its California predecessor,[92] obliges a database possessor to exercise care to protect the personal information of data subjects.[93] However, unlike the California SBIA,[94] the Texas act does not create a civil cause of action against a database possessor who fails to exercise reasonable care. Indeed, while the Texas act is silent on that subject, it expressly provides for a deceptive trade practices action[95] against hackers and others who "obtain, possess, transfer, or use [the] personal identifying information of another" without authorization.[96] It would be reasonable to interpret the Texas statute as an expression that civil liability should extend only to hackers and other unauthorized persons, and not to database possessors. *Expressio unius est exclusio alterius*.[97] Public policy could support that construction of the law because

---

87. *See* Rhode Island Identity Theft Protection Act of 2005, ch. 225, sec. 1, § 11-49.2-2(2), 2005 R.I. Gen. Laws Adv. Legis. Serv. (LexisNexis), *available at* 2005 R.I. ALS 225 (LexisNexis) ("A business that owns or licenses computerized unencripted personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."). Each violation of the Rhode Island law "is a civil violation for which a penalty of not more than a hundred dollars ($100) per occurrence and not more than twenty-five thousand dollars ($25,000) may be adjudged against a defendant."). *Id.* § 11-49.2-6(A).

88. Personal Information Protection Act, ARK. CODE ANN. §§ 4-110-101 to -108 (Supp. 2005). The Act requires a "person or business that acquires, owns, or licenses personal information about an Arkansas resident . . . [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." *Id.* § 4-110-104(b).

89. *Id.* § 4-110-108.

90. *Id.* § 4-110-106(b) (emphasis added).

91. Identity Theft Enforcement and Protection Act, ch. 294, sec. 2, §§ 48.001 to -.203, 2005 Tex. Sess. Law Serv. (West), *available at* TX LEGIS 294 (2005) (Westlaw).

92. CAL. CIV. CODE § 1798.81.5(b) (West Supp. 2005).

93. Identity Theft Enforcement and Protection Act § 48.102(A) ("A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business . . . .").

94. *See* CAL. CIV. CODE § 1798.84(b).

95. Identity Theft Enforcement and Protection Act § 48.203.

96. *See* Identity Theft Enforcement and Protection Act § 48.101 (providing that "[a] person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name").

97. "A canon of construction holding that to express or include one thing implies the exclusion of the other, or of the alternative." BLACK'S LAW DICTIONARY 620 (8th ed. 2004).

judicial deference to a coequal branch of government[98] means that a court should not create a cause of action where the legislature has implicitly determined that none should exist.[99]

C. Basic Tort Principles

1. Palsgraf*,* Kline*, and Related Cases*

Turning to the issue of whether common law principles—as opposed to statutes—support judicial recognition of a database possessor's duty to safeguard information from intruders, two landmark cases offer guidance: *Palsgraf v. Long Island Railroad Co*.[100] and *Kline v. 1500 Massachusetts Avenue Apartment Corp*.[101] These decisions have appeared in countless tort casebooks, and judicial decisions have cited them scores of times. *Palsgraf* and *Kline* are important pillars in the temple of American tort law.

In *Palsgraf*, the most famous tort case of all time, the majority opinion was written by Chief Judge Benjamin Cardozo, the "most justly celebrated of American common-law judges."[102] Cardozo set down the basic rule on duty for the New York Court of Appeals: "The risk reasonably to be perceived defines the duty to be obeyed, and risk imports relation; it is risk to another or to others within the range of apprehension."[103] In *Palsgraf*, nothing in the appearance of a newspaper-wrapped package carried by a man trying to board a moving train gave notice that the parcel contained explosives.[104] Therefore, nothing warned the trainmen that Helen Palsgraf, a patron waiting across the platform, was in danger.[105] There was no "risk [to her] reasonably to be perceived" and thus no "duty [to her] to be obeyed."[106] So far as she was concerned, the railroad had no legal obligation not to carelessly dislodge the package while trying to assist the man who was running for the train

---

98. *See* JOHNSON & GUNN, *supra* note 38, at 9 (noting that it is a policy foundation of American tort law that "[c]ourts should accord due deference to co-equal branches of government"; "there are occasions when the judiciary should eschew action in favor of other branches . . . . [C]ertain questions are best left to the legislature because of its ability to gather facts through the legislative hearing process, to craft comprehensive solutions to broad-ranging questions, or to represent the will of the public on highly controversial issues" (emphasis omitted)).

99. *Cf.* Bruegger v. Faribault County Sheriff's Dep't., 497 N.W.2d 260, 262 (Minn. 1993) (holding that violation of the Crime Victims Reparations Act (CVRA) does not create private cause of action against law enforcement agencies when the agencies failed to inform the plaintiffs of their rights to seek reparations. "Principles of judicial restraint preclude us from creating a new statutory cause of action that does not exist at common law where the legislature has not either by the statute's express terms or by implication provided for civil tort liability.").

100. 162 N.E. 99 (N.Y. 1928).

101. 439 F.2d 477 (D.C. Cir. 1970).

102. JOHN T. NOONAN, JR., PERSONS AND MASKS OF THE LAW: CARDOZO, HOLMES, JEFFERSON, AND WYTHE AS MAKERS OF THE MASKS 111 (1976).

103. *Palsgraf*, 162 N.E. at 100.

104. *Id.* at 99.

105. *Id.*

106. *Id.* at 100.

"but seemed unsteady as if about to fall."[107] Because no duty ran to Palsgraf, the railroad was not liable in negligence for the harm she sustained when the package fell and exploded.[108]

Courts today continue to apply the *Palsgraf* duty rule.[109] Thus, it is useful to ask whether, from the standpoint of database possessors, there is a "risk reasonably to be perceived"[110] to data subjects if data is not protected from unauthorized intrusion. Obviously, in many situations (such as where hackers can access data via the Internet), the answer is "yes." The risk is entirely foreseeable, and a threat to the interests of data subjects is "within the range of apprehension."[111] At least on its face, the basic rule in *Palsgraf* suggests that database possessors should often have a duty to exercise reasonable care to protect data from intruders.

Palsgraf did not involve the threat of criminal intervention, but *Kline* did.[112] In *Kline*, a landlord was on notice that "an increasing number of assaults, larcenies, and robberies [were] being perpetrated against the tenants in and from the common" areas of a large apartment building.[113] In holding the landlord responsible for a subsequent attack on the plaintiff, the court said that a landlord is by no "means an insurer of the safety of his tenants" and is not obliged "to provide protection commonly owed by a municipal police department."[114] However, a landlord is under a duty to take such precautions as "are within his power and capacity to take" in order to prevent harm by criminal intruders.[115] In writing for the District of Columbia Circuit, Judge Malcolm Richard Wilkey emphasized the fact that the landlord was the only party in a position to secure the common areas:

> No individual tenant had it within his power to take measures to guard the garage entranceways, to provide scrutiny at the main entrance of the building, to patrol the common hallways and elevators, to set up any kind of a security alarm system in the building, to provide additional locking devices on the main doors, to provide a system of announcement for authorized visitors only, to close the garage doors at appropriate hours, and to see that the entrance was manned at all times.[116]

---

107. *Id.* at 99.

108. Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 101 (N.Y. 1928).

109. *See, e.g.*, Holder v. Mellon Mortgage Co., 5 S.W.3d 654, 654–58 (Tex. 1999) (deciding, with reliance on *Palsgraf*, that the owner of a parking garage was not responsible for an attack perpetrated there on a third person by a stranger in the middle of the night because the owner had no reason to foresee that the victim would be present at that hour).

110. *Palsgraf*, 162 N.E. at 100.

111. *Id.*

112. Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970).

113. *Id.* at 479.

114. *Id.* at 486–88.

115. *Id.* at 487 (stating that a landlord's "duty is to take those measures of protection which are within his power and capacity to take, and which can reasonably be expected to mitigate the risk of intruders assaulting and robbing tenants").

116. *Id.* at 480.

The court added:

> The landlord is entirely justified in passing on the cost of increased protective measures to his tenants, but the rationale of compelling the landlord to do it in the first place is that he is the only one who is in a position to take the necessary protective measures for overall protection of the premises . . . .[117]

A similar analysis is equally applicable to cases involving database security. Individual data subjects are in a poor position to protect database information from intruders.[118] The database possessor, in contrast, is the only one with the ability to mitigate the risk that intruders may cause harm. As in *Kline*, the database possessor can spread the cost of providing database security to a broader class of data subjects, at least in cases where there is customer relationship between the plaintiff and defendant. *Kline*, like *Palsgraf*, suggests that, at least in some circumstances, database possessors should owe data subjects a duty to exercise reasonable care to protect data from intruders.

In both *Palsgraf* and *Kline*, there was a relationship between the plaintiff and the defendant. Palsgraf was a ticket purchaser of the defendant railroad;[119] Kline was a tenant of the defendant corporation.[120] Those relational ties are important, for other cases teach that duty often depends upon more than foreseeability of harm and opportunity to take precautions—it depends, sometimes, on a special linkage between the party who owes the duty and the one who receives its benefit. In this regard, recent cases involving allegedly negligent enablement of imposter fraud[121] are instructive.

---

117. *Id.* at 488.

118. *Cf.* White, *supra* note 4, at 852–53 ("Frequently, an individual does not know how much information is stored in his digital dossier, or who has compiled it. This makes it difficult, if not impossible, for an individual to control access to his personal information and, thus, limit his vulnerability to instances of identity theft.").

119. Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 99 (N.Y. 1928).

120. Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 478–79 (D.C. Cir. 1970).

121. *See generally* Brendan Delany, Comment, *Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Imposter Fraud*, 54 CATH. U. L. REV. 553, 556 (2005) (arguing for "greater federal protection for potential victims of identity theft and for common law judicial recognition of the tort of negligent enablement of impostor fraud").

In *Huggins v. Citibank, N.A.*,[122] for example, the plaintiff sued various banks on the ground that they "negligently issued credit cards" in the plaintiff's name to an "unknown imposter."[123] The plaintiff alleged, among other things, that the banks issued "credit cards without any investigation, verification, or corroboration" of the applicant's identity.[124] In response, "the [b]anks asserted they owed no duty to [the plaintiff] because he was not their customer."[125] The court agreed with the defendants and wrote:

> In order for negligence liability to attach, the parties must have a relationship recognized by law as the foundation of a duty of care. In the absence of a duty to prevent an injury, foreseeability of that injury is an insufficient basis on which to rest liability. . . .
>
> . . . .
>
> . . . The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.[126]

Other courts have reached similar conclusions.[127]

Together, *Palsgraf*, *Kline*, and *Huggins* indicate that the strongest cases for imposing a common law duty to guard data from intruders will be those in which there is a business relationship[128] between the defendant database possessor and the plaintiff data subject. This conclusion makes sense on economic as well as doctrinal grounds. Imposing a duty of care in these cases will force the database possessor, who benefits from the use of computerized information, to internalize losses relating to improperly accessed data as a cost of doing business.[129] That duty will

---

122. 355 S.C. 329, 585 S.E.2d 275 (2003).

123. *Id.* at 331, 585 S.E.2d at 276.

124. *Id.*

125. *Id.* at 332, 585 S.E.2d at 276.

126. *Id.* at 333–34, 585 S.E.2d at 277 (citations omitted).

127. *See, e.g.*, Smith v. Citibank, N.A., No. 00-0587-CV-W-1-ECF, 2001 WL 34079057, at *2–4 (W.D. Mo. Oct. 3, 2001) (holding the credit card issuer was not liable in negligence to a non-customer); Polzer v. TRW, Inc., 682 N.Y.S.2d 194, 195 (N.Y. App. Div. 1998) ("[P]laintiffs . . . failed to state a cause of action in negligence, because [the defendants] had no special relationship either with the impostor who stole the plaintiffs' credit information and fraudulently obtained credit cards, or with plaintiffs, with whom they stood simply in a creditor/debtor relationship.").

128. Sometimes parties may propose, but not consummate, a business relationship, such as when an applicant applies to a university but is not accepted for admission. The business (university) benefits from the solicitation and review of applications, so it may be fair to impose an obligation on the institution to safeguard the data of the applicant for as long as the institution retains that data. The same would seem to be true when the relationship has effectively ended, as in the case of a student who has graduated. *Cf.* Stacy Finz, *Rohnert Park; Hackers Hit College Computer System, Identity Theft Fears at Sonoma State*, S.F. CHRON., Aug. 9, 2005, at B2 (discussing hackers who gained access to the records of 61,709 persons "who either attended, applied, graduated or worked" at Sonoma State University).

129. *See* JOHNSON & GUNN, *supra* note 38, at 7–8 ("It has often been urged that . . . . [t]hose who benefit from dangerous activities should bear resulting losses. Certain activities—*e.g.*, owning a dog that may bite or using explosives—entail a serious risk of harm to third persons even if care is exercised by the actor. According to this principle, fairness requires that those who enjoy the benefits of such conduct should bear resulting losses . . . . In a related vein, it is sometimes said that an activity 'must

in turn create an incentive for database possessors to scrutinize whether their business methods are really worth the costs they entail. At the same time, the imposition of a duty in a business context gives the database possessor a means for distributing the loss by adjusting the price of the goods or services it sells to the class of persons that ultimately benefits from the defendant's business methods. That reallocation of losses will help ensure that the costs relating to improperly accessed data will not fall with crushing weight on either the data subject or the database possessor.[130]

2. Public Policy Analysis

In addressing questions of duty in unsettled areas of the law,[131] courts often ask whether imposition of duty makes sense as a matter of public policy. They consider, for example, whether obligating the defendant to exercise care would tend to minimize harm to potential plaintiffs without being unduly burdensome to the defendant or disruptive to the community.[132] Courts sometimes also consider "the availability, cost, and prevalence of insurance for the risk involved,"[133] with the assumption being that insurability of the risk makes imposition of a duty more palatable because of the cost-spreading ability of insurance. On each of these grounds—deterrence of losses, burden to the defendant, community consequences, and insurance—a good argument exists for requiring database possessors to exercise care to prevent harm by intruders.

Placing a burden on database possessors to protect data from unauthorized access would tend to reduce intruder-related losses by encouraging investment in database security.[134] That investment would be consistent with the possessors' own interests because unauthorized access entails huge costs for those who maintain databases.[135] Companies must spend large sums of money to protect their

---

pay its own way.' What this means is that there is good reason for the law to force the promoters of activities to 'internalize' the costs that their endeavors inflict on third persons. Only when those costs are taken into account, it is argued, are promoters likely to make decisions that are not only personally beneficial, but socially responsible." (emphasis omitted)).

130. *But see id.* at 743 (discussing the limits of risk spreading).

131. *Cf.* Rustad, *supra* note 3, at 108 ("It is unclear . . . whether a website owes a general duty of care to website visitors when there is no statutorily mandated standard of care.").

132. *See* Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968) (indicating that among the policy considerations typically deemed relevant to whether a duty to act should be imposed are "the moral blame attached to the defendant's conduct, the policy of preventing future harm, [and] the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach").

133. *Id.*

134. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 45 ("If tort law is found to apply to computer security, then the potential for civil liability lawsuits (with the likelihood of monetary damages) could encourage companies to invest in computer security measures.").

135. *See* Wible, *supra* note 16, at 1578 ("Even a nonmalicious trespass disrupts the victim's online services while the breach is fixed. . . . [C]ompanies generally expend resources investigating the matter, often hiring private investigators so that they do not suffer reputational loss.").

websites[136] and other data sources, and to cover resulting harm when protection efforts are unsuccessful.[137] "The financial losses facing corporate America as a result of network security breaches are staggering—hundreds of millions, if not billions, of dollars each year."[138] The burden resulting from the imposition of a legal duty would by no means be solely for the benefit of potential plaintiffs.

The imposition of a common law tort duty to protect databases would also be consistent with the developing fabric of the law. As the preceding discussion suggests, an increasing number of statutes[139] and regulations,[140] as well as commentators,[141] say that database possessors must exercise reasonable care to protect computerized personal data from unauthorized access. Thus, recognition of a tort duty to protect data would not be disruptive to the community. The duty would not require new institutions or controversial practices. Indeed, a common law tort duty to protect data would complement recent developments in both law and business.

Insurance can spread the liability risks arising from data intrusion,[142] and insurance companies are now offering these policies.[143] Of equal importance, insurers can and do provide guidance to their insureds about practices calculated

---

136. *See* Rustad, *supra* note 3, at 100 ("In 2000, private companies spent an estimated $300 billion in private enforcement efforts against hackers and viruses.").

137. *See* Wible, *supra* note 16, at 1597–98 (reporting that "[c]omputer crime cost about $250 million in 1998 and jumped to more than $375 million in 2001." (footnotes omitted)).

138. *See* Steinberg, *supra* note 26, at 60.

139. Presumably, the existence of state security breach notification laws increases judicial willingness to recognize a common law duty to protect databases. *Cf.* Paetkau & Torabian-Bashardoust, *supra* note 46, at 39 (discussing the obligation under California law to disclose security breaches and opining that "from a legal perspective, if the company notifies only California residents of a security breach, potentially affected non-Californian residents could persuasively argue that the company was at least negligent in not notifying them of the breach").

140. *See supra* Part II.B.1 (discussing the regulations adopted pursuant to the GLBA).

141. *See* Erin Kenneally, *Stepping on the Digital Scale: Duty and Liability for Negligent Internet Security*, 1 Ann. 2002 ATLA-CLE 403 (2002) (discussing the liability of companies doing business on the web).

142. *See* JOHNSON & GUNN, *supra* note 38, at 7 (noting that in the development of American tort law it has often been urged that "[t]he costs of accidents should be spread broadly. The idea underlying the 'spreading' rationale is that the financial burden of accidents may be diminished by spreading losses broadly so that no person is forced to bear a large share of the damages. . . . Losses can be spread not only through increases in the costs of goods and services, but through other devices such as taxation and insurance" (emphasis omitted)).

143. *See* Steinberg, *supra* note 26, at 60 (stating that "[s]tand-alone network-risk, hacker, or cyber insurance is now being offered . . . . [T]hese policies offer protection against intangible data loss from viruses, denial-of-service attacks, and theft of consumer information—and the protection can extend to third-party liabilities. Insurance premiums remain considerable, and prequalifying security assessments can be demanding; moreover, legal advice is often a pre-requisite for navigating the various gaps and exclusions written into such policies").

to minimize liability.[144] That advice helps to reduce the frequency and amount of future losses, thereby reinforcing the deterrence objectives of the law.

Imposing a tort duty under which database possessors will be liable for negligent data security practices will inevitably leave many questions unanswered. To say that an enterprise has a duty to exercise reasonable care to ensure data security provides no clear guidance as to practical questions, such as how often patches should be applied to security software.[145] But these types of questions are no different than those that courts face in a thousand other settings when they apply the rules of negligence liability. Over the long run, the burden of uncertainty will be minimized by evolving guidance found in scholarship discussing court decisions and legislation,[146] the development of industry customs,[147] and the promulgation of regulations which help define conduct required of a potential defendant seeking to avoid liability.

3. Voluntary Assumption of Duty

Even if courts decline to impose a tort duty to safeguard data on database possessors generally (or at least on businesses), voluntary-assumption-of-duty principles may create a legally enforceable data-protection obligation.[148] A person not otherwise under a duty to exercise reasonable care may voluntarily assume the responsibility to do so. One way of voluntarily assuming this duty is by promising to exercise care and thereby inducing detrimental reliance.[149] Another way is by "undertak[ing] to render services" and consequently increasing the risk of harm to the plaintiff.[150] Either way, the party who undertook the duty of reasonable care will

144. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 65–66 (discussing how the insurance industry can motivate responsible practices in the private sector); Jay P. Kesan, Rupterto P. Majuca, & William J. Yurcik, *The Economic Case for Cyberinsurance* 19 (Univ. of Ill. Coll. of Law, Working Paper No. 2, 2004), *available at* http://ssrn.com/abstract=577862 (stating that cyberinsurance "companies can . . . facilitate standards for best practices by calibrating the amount of IT security they require the insured to possess to socially-optimal levels").

145. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 51 (discussing the practical problems that may arise from a duty to exercise reasonable care to ensure data security).

146. *See* Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SEDONA CONF. J. 109, 109 (discussing "laws and regulations requiring security" and "the developing trend as to what businesses must do to satisfy their legal obligations to provide appropriate security").

147. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 50 ("As a motivating factor for industry to adopt best practices, tort law can be a significant complement to standard-setting, because compliance with industry-wide standards is usually an acceptable demonstration of due care."); Randy V. Sabett, *Graceful Disclosure: The Pros & Cons of Mandatory Reporting of Security Vulnerabilities*, 4 SEDONA CONF. J. 121, 124 (2003) (stating that "several organizations have developed vulnerability disclosure policies" relating to software).

148. *See generally* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 42 (Proposed Final Draft No. 1, 2005) (discussing duty based on undertaking).

149. *See id.* § 42 cmt. e (discussing promises as undertakings).

150. *See id.* § 42 ("An actor who undertakes to render services to another that the actor knows or should know reduce the risk of physical harm to the other has a duty of reasonable care to the other in conducting the undertaking if . . . the failure to exercise such care increases the risk of harm beyond that which existed without the undertaking.").

be subject to liability if it breaches the voluntarily assumed duty and causes damages.

These well-established principles might apply to situations where consumers reveal personal information to financial institutions in reliance on financial institutions' stated privacy policies.[151] For example, the policy of one major banking institution, which is not atypical, states in reassuring terms:

> The law gives you certain privacy rights. Bank of America gives you more.
>
> . . . .
>
> Keeping financial information secure is one of our most important responsibilities. We maintain physical, electronic and procedural safeguards to protect Customer Information.
>
> . . . .
>
> . . . All companies that act on our behalf are contractually obligated to keep the information we provide to them confidential . . . .[152]

A customer reading this information would conclude, at a minimum, that in exchange for entrusting the bank with personal information, the bank agreed (1) to protect the data by means of physical, electronic, and procedural safeguards and (2) to keep it confidential. Other language in the privacy policy reinforces those sensible conclusions by stressing the importance of precautions on the part of the customer to guard against disclosure or unauthorized use of account and personal information.[153] The same is true of statements in the bank's advertising[154] and on its website emphasizing the dangers of identity theft and assuring the customer that "[y]our checking account statements are always protected in Online Banking."[155] A court might reasonably interpret such a privacy policy as an undertaking to exercise reasonable care, and might conclude that a breach of that duty would support a tort cause of action.

Similarly, even if the plaintiff never read or relied on the institution's privacy policy, a court might impose a duty of care under the other prong of the undertaking rule, which says where services provided for the protection of another increase the risk of harm "beyond that which existed without the undertaking," there is a duty

---

151. *See generally* Therese G. Franzén & Leslie Howell, *Financial Privacy Rules: A Step By Step Guide to the New Disclosure Requirements Under the Gramm-Leach-Bliley Act and the Implementing Regulations*, 55 CONSUMER FIN. L.Q. REP. 17, 20-21 (2001) (discussing privacy notices).

152. Bank of America, Privacy Policy for Consumers 2005, http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr (last visited Nov. 15, 2005).

153. *See id.*

154. *See* Dash, *From Data Holders*, *supra* note 14 (reporting that "financial services and technology companies have been quietly tweaking their advertising to incorporate themes about the safety of customers' data").

155. Bank of America, Online Banking, http://www.bankofamerica.com/privacy/index.cfm?template =privacysecure_olb (last visited Oct. 30, 2005).

to exercise reasonable care.[156] Depending on the facts, the measures taken to protect computerized data (e.g., use of passwords and firewalls) may contain flaws that increase the risk of unauthorized data access. An increased risk of harm might also result when data protection practices allow transmission of unencrypted data, which is especially vulnerable to hacking. The increased-risk rule might apply in these types of cases.

According to the *Restatement* provision on undertakings, negligence liability based on inducing detrimental reliance or increasing the risk of injury is limited to compensation for physical harm.[157] This significant limitation presumably means that the economic losses associated with identity theft are not recoverable under this theory of duty. However, a database possessor might still be liable under the undertaking rule for personal injury or property damage perpetrated on a data subject by an intruder or one who obtained personal information from the intruder.

D. Fiduciary Obligations

A fiduciary is one who voluntarily[158] holds a position of special trust and confidence that obliges the fiduciary to act in the best interest of another.[159] The duties imposed on a fiduciary—including loyalty, candor, and confidentiality—are sometimes coextensive with those that the law of negligence embraces.[160] However, depending on the circumstances, fiduciary obligations may extend considerably further than a duty of reasonable care.[161]

If a database possessor owes fiduciary obligations to a data subject, it is reasonable to argue that regardless of whether general tort principles would impose a duty, the fiduciary is obliged to protect computerized information relating to the data subject from unauthorized access by third parties.[162] For example, the

---

156. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 42(a) (Proposed Final Draft No. 1, 2005) (discussing increased risk of harm).

157. *See id.* § 42 cmt. a.

158. *See* PulseCard, Inc. v. Discover Card Servs., Inc., 917 F. Supp. 1478, 1484 (D. Kan. 1996) (stating that "[t]he hallmark of a fiduciary relationship is a voluntary and conscious assumption or acceptance of the duties of a fiduciary").

159. *See* RESTATEMENT (SECOND) OF TORTS § 874 cmt. a (1979) (stating that "[a] fiduciary relation exists between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation").

160. *See* Vincent R. Johnson & Shawn M. Lovorn, *Misrepresentation by Lawyers About Credentials or Experience*, 57 OKLA. L. REV. 529, 544 (2004) (noting that while "[s]ome courts have said that attorneys owe clients a duty of 'absolute and perfect candor'[,] . . . [that] is an overstatement of an attorney's disclosure obligations, for in many contexts the law imposes no more than a duty of reasonable care to keep a client informed of relevant matters").

161. *See* Vincent R. Johnson, *"Absolute and Perfect Candor" to Clients*, 34 ST. MARY'S L.J. 737, 792 (2003) [hereinafter *Candor*] (indicating that if the interests of lawyer and client diverge, the lawyer's duty is essentially one of absolute and perfect candor).

162. Fiduciary-duty principles come from many areas of the law, including the rules governing trusts, corporations, and agency. At least in some contexts, a breach of fiduciary duty is treated as a type of tort. *See* RESTATEMENT (SECOND) OF TORTS § 874 (1979) (stating that "[o]ne standing in a fiduciary relation with another is subject to liability to the other for harm resulting from a breach of duty imposed by the relation").

relationship between an attorney and client is fiduciary as a matter of law.[163] Accordingly, lawyers have a special fiduciary obligation to protect confidential client information, aside from any demands imposed by ordinary tort principles. A lawyer's broad fiduciary obligation of confidentiality extends to all forms of information about the client,[164] including computerized data,[165] as well as information contained in printed documents or otherwise known by the attorney,[166] for the existence of the duty turns on the content, and not the form, of the information.[167] In light of the fiduciary-duty rules on confidentiality (and the related obligations requiring safekeeping of client property[168]), a lawyer or law firm could not plausibly argue that there is no duty to safeguard computerized client data from intruders.

---

163. *See, e.g.*, Keywell Corp. v. Piper & Marbury, L.L.P., No. 96-CV-066OE (SC), 1999 WL 66700, at *4 (W.D.N.Y. Feb. 11, 1999) (stating that "[i]t is axiomatic that the relationship between an attorney and his or her client is a fiduciary one").

164. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 59 (2000) (providing that "[c]onfidential client information consists of information relating to representation of a client, other than information that is generally known").

165. *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. No. 782 (2004) ("When a lawyer sends a document by e-mail, as with any other type of communication, a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information. . . . Reasonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission."). *See generally* David Hricik, *The Speed of Normal: Conflicts, Competency, and Confidentiality in the Digital Age*, 9 COMPUTER L. REV. & TECH. J. ____ (forthcoming 2005) (discussing ethical obligations of attorneys relating to digitally stored client confidences); Jonathan Bick, *Client Internet Services Expose Firms to New Liability*, N.J. L.J., Sept. 20, 2004, *available at* http://www.bicklaw.com/Publications/Client_internet_to_Liability.htm (indicating that client services now include "offering clients protected access to their personal case information over the Internet" and stating that "ethical rules . . . [are] equally applicable to Internet transactions").

166. *See* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 643 (1993) (stating that client "files should be stored in a secure location").

167. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 60 cmt. d (2000) ("A lawyer who acquires confidential client information has a duty to take reasonable steps to secure the information against misuse or inappropriate disclosure . . . . This requires that client confidential information be acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality."); *see also* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 95-398 (1995) ("A lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information."); *cf.* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) ("Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. . . . [and] therefore . . . its use is consistent with the duty . . . to use reasonable means to maintain the confidentiality of information relating to a client's representation.").

168. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 44 (2000) (discussing the duty to safeguard and segregate client property).

The same analysis should apply to all fiduciary relationships,[169] including those that are fiduciary as a matter of law (such as trustee-beneficiary[170]) and others that are fiduciary as a matter of fact because they entail a high degree of trust and confidence.[171] Importantly, however, ordinary business relationships are not fiduciary.[172] In business, parties normally deal with one another at arm's length.[173] The "mere acceptance of confidential information" does not create a fiduciary relationship,[174] nor does the fact that one party "trusts another and relies on a promise to carry out a contract."[175] Fiduciary relationships are the exception, not the rule. Even the relationship between a teacher and a student,[176] or a university and its alumni,[177] is usually not fiduciary in nature. Consequently, while fiduciary-duty law may play an important role in determining whether professionals—such as lawyers, physicians, or trustees—have a duty to protect the information of clients, patients, and beneficiaries from intruders, it will not set the standard of care in most commercial settings.

III. THE DUTY TO REVEAL EVIDENCE OF SECURITY BREACHES

It is important to distinguish the duty to protect data from intrusion from the duty to disclose information regarding an actual breach in data security. A statute might impose both of these obligations (as does California's SBIA),[178] or it might impose one duty but not the other. For example, the Louisiana Database Security

---

169. *Cf.* PulseCard, Inc. v. Discover Card Servs., Inc., 917 F. Supp. 1478, 1484 (D. Kan. 1996) (stating that "almost every fiduciary relationship implies some duty of confidentiality").

170. *See id.* at 1483 (discussing fiduciary relationships "specifically created by contract such as principal/agent, attorney/client, and trustee/cestui que trust"); RESTATEMENT (SECOND) OF TORTS § 874 cmt. b (1979) (referring to trustee, guardian, executor, and administrator).

171. *See* Martinelli v. Bridgeport Roman Catholic Diocesan Corp., 196 F.3d 409, 429 (2d Cir. 1999) (holding that "irrespective of the duties of the Diocese to its parishioners generally, the jury could reasonably have found that the Diocese's relationship with [the plaintiff] . . . was of a fiduciary nature"); Curl v. Key, 316 S.E.2d 272, 274–76 (N.C. 1984) (reversing and remanding a lower court's determination that a confidential relationship did not exist where the defendant, who the plaintiffs referred to as "uncle" and who was the best friend of their deceased father, secured the plaintiffs' signatures on a "peace paper"); Navistar Int'l Transp. Corp. v. Crim Truck & Tractor Co., 791 S.W.2d 241, 242 (Tex. Ct. App. 1990) (indicating that informal relationships may be fiduciary).

172. *See, e.g.*, *PulseCard, Inc.*, 917 F. Supp. at 1484, 1488 (stating that "fiduciary obligations should be extended reluctantly to commercial or business transactions" and holding that a relationship between a credit card company and a provider of transaction processing services was not fiduciary).

173. *See* Pellegrini v. Cliffwood-Blue Moon Joint Venture, Inc., 115 S.W.3d 577, 580 (Tex. Ct. App. 2003) (characterizing the relationship between a geophysicist contractor and a joint venture as an arm's-length transaction).

174. *PulseCard, Inc.*, 917 F. Supp. at 1485.

175. *See Navistar*, 791 S.W.2d at 243.

176. *See* Ho v. Univ. of Tex. at Arlington, 984 S.W.2d 672, 693 (Tex. Ct. App. 1998) (holding there is no fiduciary relationship "between teachers and students in a normal educational setting").

177. *See* Brzica v. Trs. of Dartmouth Coll., 791 A.2d 990, 994–95 (N.H. 2002) (holding the facts did not establish a fiduciary relationship between college trustees and alumni).

178. *See* CAL. CIV. CODE § 1798.81.5(b) (West Supp. 2005) (specifying a duty to "implement and maintain reasonable security procedures and practices"); *id.* § 1798.82(a) (imposing a duty to disclose "any breach of security of the system").

Breach Notification Law[179] does not create an explicit duty to protect data, but requires notification of data subjects upon discovery of a security breach.[180] In addition, common law rules may distinguish the duty to disclose from the duty to protect. Under certain rules, one whose conduct, "even though not tortious, creates a continuing risk of physical harm" to the plaintiff "has a duty to exercise reasonable care" to prevent the harm from occurring or to minimize the adverse consequences.[181] Even if a database possessor was not under a duty enforceable in a private action to protect a data subject's personal information from unauthorized access, an intrusion may impose a duty on the database possessor to reveal the breach in security.[182]

There are at least four ways of imposing on potential defendants a duty to reveal a compromise in database security. First, a statute may impose a duty, either as a result of the statute's express terms or as a result of judicial reliance on the statute as the proper expression of the standard of care.[183] Second, a duty may arise from common law principles governing negligence liability generally.[184] Third, there may be a duty under law of misrepresentation, which imposes a general duty to update previously accurate statements (e.g., statements relating to data security) that are the basis for pending or continuing reliance by the recipient of the statements.[185] Finally, failure-to-act rules may require the exercise of reasonable care to avoid or minimize damages if a database possessor's conduct created a continuing risk of physical harm.[186]

A. Statutory Duties

At least eighteen states[187] have adopted database security breach information acts that require certain types of database possessors (typically businesses,[188] but

---

179. Database Security Breach Notification Law, ch. 51, §§ 3071-77, 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw).

180. *Id.* § 3074(A).

181. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1, 2005).

182. *See infra* Part III.B.3.

183. *See infra* Part III.A.

184. *See infra* Part III.B.1.

185. *See infra* Part III.B.2.

186. *See infra* Part III.B.3.

187. *See supra* note 29.

188. *See, e.g.*, MONT. CODE ANN. §§ 30-14-1702(1)(a), -1704(1)–(2) (2005) (imposing a notification obligation on "[a]ny person or business that conducts business" and defining a business as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution . . . or the parent or the subsidiary of a financial institution."); N.D. CENT. CODE § 51-30-02 (Supp. 2005) (imposing a notification obligation on "[a]ny person that conducts business"). *But see* GA. CODE ANN. §§ 10-1-911(2), –912(a) (Supp. 2005) (limiting the obligation to "information brokers," who are "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties," and not including "any governmental agency whose records are maintained

sometimes governmental agencies[189] or other persons or entities,[190] such as non-profit organizations[191]) to notify data subjects of violations (or possible violations) of their information's security.[192] Several of the states that impose notification obligations expressly authorize a civil action for damages.[193] In addition, Illinois

---

primarily for traffic safety, law enforcement, or licensing purposes"); Act to Protect Maine Citizens from Identity Theft, ch. 379, sec. 1, § 1348(1), 2005 Me. Legis. Serv. (West), *available at* ME LEGIS 379 (Westlaw) (limiting the notification duty to information brokers). Some businesses may be exempt from state law obligations imposed on businesses generally. *See, e.g.*, Database Security Breach Notification Law, ch. 51, § 3076, 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw) (exempting financial institutions that are subject to, and in compliance with, certain federal rules).

189. *See, e.g.*, Act effective July 1, 2005, Pub. L. No. 91-2005, ch. 10, 11, sec. 1, 2, §§ 4-1-10-2, -11-5(a), 2005 Ind. Legis. Serv. (West), *available at* IN LEGIS 91-2005 (2005) (Westlaw) (limiting the notification obligation to state agencies, including state educational institutions); Act of June 17, 2005, ch. 486, sec. 2, 6, §§ 4(1), 6(1), 2005 Nev. Stat., *available at* NV LEGIS 486 (Westlaw) (imposing a duty on governmental agencies and applying separate provisions to persons "doing business"); Act of June 17, 2005, ch. 485, sec. 16, § 24, 2005 Nev. Stat., *available at* NV LEGIS 485 (2005) (Westlaw) (imposing a notification duty on "data collector"); Rhode Island Identity Theft Protection Act of 2005, ch. 225, sec. 1, §§ 11-49.2-3(A), 11-49.2-5(A), 2005 R.I. Gen. Laws Adv. Legis. Serv. (LexisNexis), *available at* 2005 R.I. ALS 225 (LexisNexis) (requiring that "[a]ny state agency or person that owns, maintains or licenses computerized data" provide notification, and defining "person" as "any individual, partnership association, corporation or joint venture"); Act of May 10, 2005, ch. 368, §§ 1(1)(a), 2(1), 2005 Wash. Legis. Serv. (West), *available at* WA LEGIS 368 (2005) (Westlaw) (imposing a notification obligation on governmental agencies and placing a similar obligation on "[a]ny person or business that conducts business in the state" through other provisions).

190. *See* Personal Information Protection Act, Pub. Act 94-36, ch. 815, sec. 530, §§ 5, 10(a)-(b), 2005 Ill. Legis. Serv. (West), *available at* IL LEGIS 94-36 (2005) (Westlaw) (imposing a notification obligation on a "data collector," which "may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information"); Act effective July 1, 2005, ch. 473, sec. 1, §§ 47-18-2107(a)(2), -2107(b), 2005-2 Tenn. Code Ann. Adv. Legis. Serv. 749, 749-50 (LexisNexis) (imposing a notification duty on an "information holder," which includes "any person or business that conducts business in this state, or any agency of the State of Tennessee or any of its political subdivisions").

191. Act of June 28, 2005, Pub. L. 61, sec. 1, §§ 12B-101(2), 12B-102, 2005 Del. Code Ann. Adv. Legis. Serv. (LexisNexis), *available at* 2005 Del. ALS 61 (LexisNexis) (imposing a notification obligation on a "'commercial entity' . . . whether for profit or not-for-profit").

192. Act of June 14, 2005, ch. 2005-229, sec. 2, § 817.5681(1)(a), 2005 Fla. Sess. Law Serv. (West), *available at* FL LEGIS 2005-229 (Westlaw) (imposing a notification obligation when any resident's personal information "was, or is reasonably believed to have been, acquired by an unauthorized person"); Act effective July 1, 2005, Pub. L. No. 91-2005, ch. 10, sec. 2, § 4-1-11-5(a), 2005 Ind. Legis. Serv. (West), *available at* IN LEGIS 91-2005 (2005) (Westlaw).

193. *See* CAL. CIV. CODE § 1798.84(b) (West Supp. 2005) (stating that "[a] customer injured by a violation of this title may institute a civil action to recover damages"); Database Security Breach Notification Law, ch. 51, § 3075, 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw) (providing that "[a] civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information."); Act of June 17, 2005, ch. 486, sec. 2, § 4(5), 2005 Nev. Stat., *available at* NV LEGIS 486 (2005) (Westlaw) (providing that "[a] person who has suffered injury as the proximate result of a violation of this section may commence an action against the governmental agency for the recovery of his actual damages, costs and reasonable attorney's fees," subject to limitations); *id.* § 6(7) ("A person who has suffered injury as the proximate result of a violation of this section may commence an action against the person doing business in this State for the

allows a deceptive trade practices action,[194] which permits a "person who suffers actual damage . . . [to recover] actual economic damages or any other relief which the court deems proper,"[195] including "reasonable attorney's fees and costs."[196] In other states, a variety of means enforce the notification obligation, such as administrative[197] or civil[198] fines, or an action by the attorney general[199] to recover "direct economic damages"[200] or to remedy deceptive trade practices.[201]

In states not expressly providing for civil liability to data subjects, an individual may be able to rely upon a notification statute that does not expressly create a private right of action as the basis for a suit alleging negligence per se.[202] State security breach notification laws, unlike the federal GLBA and related

---

recovery of his actual damages, costs and reasonable attorney's fees and, if the violation of this section was willful or intentional, for any punitive damages that the facts may warrant."); Act effective July 1, 2005, ch. 473, sec. 1, § 47-18-2107(h), 2005-2 Tenn. Code Ann. Adv. Legis. Serv. 749, 751 (LexisNexis) ("Any customer of an information holder who is a person or business entity, but who is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section may institute a civil action to recover damages . . . ."); Act of May 10, 2005, ch. 368, §§ 1(10)(a), 2(10)(a), 2005 Wash. Legis. Serv. (West), *available at* WA LEGIS 368 (2005) (Westlaw) (providing that "[a]ny customer injured by a violation of this section may institute a civil action to recover damages").

194. Personal Information Protection Act, Pub. Act 94-36, ch. 815, sec. 530, § 20, 2005 Ill. Legis. Serv. (West), *available at* IL LEGIS 94-36 (2005) (Westlaw) ("A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.").

195. 815 ILL. COMP. STAT. ANN. 505/10a(a) (West Supp. 2005).

196. *Id.* at 505/10a(c).

197. *See* Act of June 14, 2005, ch. 2005-229, sec. 2, § 817.5681(1)(b), 2005 Fla. Sess. Law Serv. (West), *available at* FL LEGIS 2005-229 (Westlaw) ("Any person required to make notification . . . who fails to do so within 45 days . . . is liable for an administrative fine not to exceed $500,000, as follows: 1. In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days. 2. If notification is not made within 180 days, any person required to make notification under paragraph (a) who fails to do so is subject to an administrative fine up to $500,000."); *id.* § 817.5681(1)(c) ("The administrative sanctions for failure to notify provided in this subsection shall apply per breach and not per individual affected by the breach."); *id.* § 817.5681(1)(d) (providing that the administrative sanctions generally do not apply against "any governmental agency or subdivision").

198. *See* MONT. CODE ANN. §§ 30-14-1705(3), -103, -142 (Supp. 2005) (providing that violations constitute deceptive trade practices subject to injunctive relief and civil fines); Rhode Island Identity Theft Protection Act of 2005, ch. 225, sec. 1, § 11-49.2-6(A), 2005 R.I. Gen. Laws Adv. Legis. Serv. (LexisNexis), *available at* 2005 R.I. ALS 225 (LexisNexis) ("Each violation of this chapter is a civil violation for which a penalty of not more than a hundred dollars ($ 100) per occurrence and not more than twenty-five thousand dollars ($ 25,000) may be adjudged against a defendant.").

199. *See* Act of June 2, 2005, ch. 167, sec. 1, § 6, 2005 Minn. Sess. Law Serv. (West), *available at* MN LEGIS 167 (2005) (Westlaw) (providing that "[t]he attorney general shall enforce this section").

200. *See* Act of June 28, 2005, Pub. Act 61, sec. 1, § 12B-104, 2005 Del. Code Ann. Adv. Legis. Serv. (LexisNexis), *available at* 2005 Del. ALS 61 (LexisNexis) ("[T]he Attorney General may bring an action in law or equity to . . . ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both.").

201. *See* Act of June 24, 2005, Pub. Act 05-148, § 3(g), 2005 Conn. Legis. Serv. (West), *available at* CT LEGIS P.A. 05-148 (Westlaw) (providing, apparently as the sole remedy, that "[f]ailure to comply with the requirements of this section shall constitute an unfair trade practice . . . and shall be enforced by the Attorney General"); *see also* 815 ILL. COMP. STAT. ANN. 505/3 to 505/7 (West 1999 & Supp. 2005) (describing the powers of the Illinois Attorney General).

202. *See supra* Part II.B (discussing general principles of negligence per se).

regulations,[203] may be sufficiently specific to avoid allegations that they are too vague to set the standard of care. These laws require prompt action and typically spell out in detail how database possessors should provide notification.[204] However, the laws do allow some flexibility.

State notification statutes often permit database possessors to adopt their own notification procedures that comply with the notice and timing requirements of the statute.[205] They also allow for a delay in notification to accommodate the needs of law enforcement[206] or other important considerations. For example, the Illinois Personal Information Protection Act[207] requires that "notification shall be made in the most expedient time possible and without unreasonable delay, *consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system*."[208] However, this type of language does not question whether a duty exists, but simply allows for a nuanced analysis of whether there has been a breach.

More importantly, some of the security breach notification laws create unlikelihood-of-harm exceptions to the disclosure obligation. For example, the Connecticut law states that "notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."[209] The Florida law requires the determination to "be documented in writing and the documentation must be maintained for 5 years."[210] These types of exceptions limit the utility of a negligence per se analysis in some states. Under this type of law, a defendant's reasonable determination that there was

---

203. *See supra* Part II.B.1 (discussing the federal GLBA and related regulations).

204. *See, e.g.*, ARK. CODE ANN. § 4-110-105 (West Supp. 2005) (detailing the acceptability of various methods of providing notice, including written notice, e-mail notice, and types of "[s]ubstitute notice").

205. *See* Act of June 28, 2005, Pub. Act 61, sec. 1, § 12B-103, 2005 Del. Code Ann. Adv. Legis. Serv. (LexisNexis), *available at* 2005 Del. ALS 61 (LexisNexis) ("[A]n individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with its policies in the event of a breach of security of the system."); *see also* GA. CODE ANN. § 10-1-911(3) (Supp. 2005) (containing similar language).

206. *See, e.g.*, GA. CODE ANN. § 10-1-912(c) (Supp. 2005) (providing that notification "may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation" and "shall be made after the law enforcement agency determines that it will not compromise the investigation").

207. Pub. Act 94-36, ch. 815, sec. 530, 2005 Ill. Legis. Serv. (West), *available at* IL LEGIS 94-36 (2005) (Westlaw).

208. *Id.* § 10(a) (emphasis added).

209. Act of June 24, 2005, Pub. Act 05-148, § 3(b), 2005 Conn. Legis. Serv. (West), *available at* CT LEGIS P.A. 05-148 (Westlaw).

210. Act of June 14, 2005, ch. 2005-229, sec. 2, § 817.5681(10)(a), 2005 Fla. Sess. Law Serv. (West), *available at* FL LEGIS 2005-229 (Westlaw); *see also id.* § 817.5681(10)(b) ("Any person [who] . . . fails to maintain the documentation for the full 5 years as required in this subsection is liable for an administrative fine in the amount of up to $50,000 for such failure.").

no likelihood of harm would presumably mean either that there was no violation of the statute as a result of non-disclosure of a security breach, or that there was an excuse for any violation that occurred.[211] Either finding would be fatal to a negligence per se action.

Some state notification statutes not expressly providing for civil liability, such as the Maine Notice of Risk to Personal Data Act,[212] appear to leave room for courts to entertain negligence per se actions by ruling out arguments that legislatures intended the statutorily created penalties[213] to be the sole measure of a database possessor's obligations.[214] The Maine Act states that "rights and remedies available under [the statute] are cumulative and do not affect or prevent rights and remedies available under federal or state law."[215]

At the federal level, Senator Dianne Feinstein has introduced legislation that would "require Federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information."[216] That bill, if adopted, would preempt inconsistent state legislation[217] but does not expressly provide that adversely affected data subjects can maintain a civil action to recover damages.[218] Another bill,[219] proposed by Senator Arlen Specter, would subject businesses maintaining records relating to 10,000 or more persons[220] to certain data protection[221] and breach notification requirements,[222] and, among other enforcement mechanisms, would allow a state attorney general to maintain an action in federal court to recover "in the sum of actual damages, restitution, and other compensation on behalf of affected residents of a State; and . . . punitive damages, if the violation is willful or intentional."[223]

---

211. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 15 cmts. a–b (Proposed Final Draft No. 1, 2005) (discussing the role of excuse in negligence per se generally).

212. Notice of Risk to Personal Data Act, ch. 379, sec. 1, § 1346, 2005 Me. Legis. Serv. (West), *available at* ME LEGIS 379 (2005) (Westlaw).

213. *Id.* § 1349(2)(A)-(C) (providing that a violation may result in "A. A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the information broker is in violation of this chapter; B. Equitable relief; or C. Enjoinment from further violations").

214. *See also* N.D. CENT. CODE § 51-30-07 (Supp. 2005) (providing that the "attorney general may enforce this chapter," but that the "remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties . . . or otherwise provided by law").

215. Notice of Risk to Personal Data Act, ch. 379, sec. 1, § 1349(3), 2005 Me. Legis. Serv. (West), *available at* ME LEGIS 379 (2005) (Westlaw).

216. S. 115, 109th Cong. (2005).

217. *Id.* § 5.

218. *Id.* § 3(b)(3).

219. Personal Data Privacy and Security Act of 2005, S. 1332, 109th Cong. (2005).

220. *Id.* § 401(b).

221. *Id.* § 402.

222. *Id.* §§ 421–22.

223. *Id.* §§ 403(b)(1)(c).

B. Basic Tort Principles

1. General Duty or Limited Duty

Part II.C discussed how general tort principles and policies can be marshaled to support judicial recognition of a duty to *protect* database information. Many of those same arguments—particularly the reasoning relating to foreseeability of danger, opportunity to prevent harm, relationship between the parties (at least in business contexts), deterrence of future losses, desirable community consequences, and the availability of insurance—have equal application to the question of whether a database possessor has a duty to *disclose* intrusion to data subjects. Those policies favor judicial recognition of a notification duty. However, determining whether the burden placed on the defendant would be too heavy to bear requires special consideration because the costs of providing notice will obviously differ from the costs of protecting a computer database.

Depending on the number of affected data subjects, the costs of notification may be substantial. Some breaches of security involve a risk to tens or hundreds of thousands of persons.[224] Notifying each of the affected individuals separately may be difficult, time consuming, and labor intensive. In addition, unlike the costs of database protection, the expense of notification does not directly benefit the database possessor.[225] Indeed, disclosure of the breach may precipitate adverse publicity and loss of business.

The states that have passed security breach notification laws have shown how to minimize the burden imposed on database possessors in some contexts through the use of alternate modes of notification.[226] The same type of alternatives—which allow for aggregate methods of communication when personal notice would be too expensive or otherwise infeasible—should be taken into account in determining whether to impose a common law notification duty and, if so, whether a database possessor has breached that duty.

A key question in determining whether to require notification is whether disclosure of the breach would be useful[227] or futile.[228] If a data subject could not

---

224. *See supra* note 14 and accompanying text.

225. However, the defendant may indirectly benefit, such as by protecting its reputation through candor.

226. *See, e.g.,* Act of June 28, 2005, Pub. Act 61, sec. 1, § 12B-101(4), 2005 Del. Code Ann. Adv. Legis. Serv. (LexisNexis), *available at* 2005 Del. ALS 61 (LexisNexis) ("'[N]otice' means: (i) written notice; (ii) telephonic notice; (iii) electronic notice, if the notice provided is consistent with [certain federal laws]; or (iv) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: a. e-mail notice . . . ; and b. conspicuous posting of the notice on the Web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and c. notice to major statewide media.").

227. "In some situations a warning is desirable because it is effective in reducing the likelihood of an accident. Yet in other situations a warning is appropriate mainly because it reduces the likely severity of the injuries that such an accident might occasion." RESTATEMENT (THIRD) OF TORTS: LIAB.

do anything to protect his or her own interests following an intrusion into data security, there would be little reason to require notification. However, individuals can act to protect themselves from financial and physical harm that persons with unauthorized access to their data may cause.[229] The federal Fair and Accurate Credit Transactions Act of 2003 (FACTA)[230] allows consumers to place a "fraud alert"[231] in the their files with credit reporting agencies. Certain state laws also enable consumers to place a "security freeze" on their credit report, which "prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer."[232] Some state laws permit victims of information security breaches to obtain a court order declaring the individual a victim of identity theft.[233] That declaration can aid the data subject in dealing with law enforcement authorities or with businesses. Consumers can also monitor their credit card and bank accounts more closely for evidence of unauthorized transactions or pay monthly service fees to a company that tracks three national credit reporting companies on a daily basis and advises subscribers of key changes to their data (such as new applications for credit by someone using the subscriber's name and identity).[234] As to physical harm, a person who has notice of a data intrusion can exercise greater caution for personal safety, if the facts so warrant.[235]

FOR PHYSICAL HARM § 18 cmt. b (Proposed Final Draft No. 1, 2005).

228. The *Restatement* indicates:

> In some situations, however, there is little or nothing a potential victim can do even if given a warning. For example, if a golfer's errant shot heads in the direction of a freeway next to the golf course, it would be pointless for the golfer to give a "fore" warning to motorists on the freeway . . . .

Id.

229. *Cf.* FDA CONSUMER, *supra* note 8 (discussing what individuals should do if they think their identity has been stolen).

230. Pub. L. No. 108–159, 117 Stat. 1952 (2003) (codified as amended in scattered sections of Titles 15 and 20 of the United States Code).

231. 15 U.S.C.A. § 1681c-1 (West Supp. 2005).

232. Act of May 9, 2005, ch. 342, § 1(1), 2005 Wash. Legis. Serv. (West), *available at* WA LEGIS 368 (2005) (Westlaw). "The consumer reporting agency . . . shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her credit report for a specific party or period of time." *Id.* § 1(4). *See also* Act of June 24, 2005, Pub. Act 05-148, § 2, 2005 Conn. Legis. Serv. (West), *available at* CT LEGIS P.A. 05-148 (Westlaw) (detailing security freeze procedures).

233. *See* Identity Theft Enforcement and Protection Act, ch. 294, sec. 2, § 48.202, 2005 Tex. Sess. Law Serv. (West), *available at* 2005 TX LEGIS 294 (2005) (Westlaw) (detailing the process to declare an individual a victim of identity theft).

234. *See* Kathleen Pender, *Credit Reports—Free for All*, S.F. CHRON., Nov. 30, 2004, at C4 (describing Experian's "credit-monitoring product, called Triple Alert," that provides customers with "same-day notification anytime someone seeks credit in their name").

235. *But see* Hayes v. State, 521 P.2d 855, 858 (Cal. 1974) (holding that there was no duty to warn students of the risk of an attack on the beach at night because "the public is aware of the incidence of violent crime, particularly in unlit and little used places" and "it would serve little purpose . . . to further remind the public of this unfortunate circumstance in society").

In many circumstances, American tort law has imposed liability for failure to warn.[236] Indeed, courts have sometimes held there is a duty to warn even when there is no duty to do anything else. For example, in many states that still follow the traditional categories relating to premises liability—trespasser, licensee, and invitee—the only duty a possessor of land owes to a licensee is to warn of dangers of which the possessor is aware.[237] Similarly, in some states, essentially the only duty of a mental health professional who knows that a patient poses a risk of harm to a third person is to warn the third person (or authorities) of the danger.[238] Consequently, it might reasonably follow that even if a state holds there is no duty to protect databases from intrusion, there should at least be a duty to provide notice of a security breach of the database.[239]

An important question remains as to how specific the notice should be that informs data subjects of unauthorized data access. In this regard, the federal Interagency Guidance[240] for financial institutions offers an informative, pro-consumer perspective. The Interagency Guidance states:

---

236. "The range of defendant conduct that can give rise to the obligation to warn is so broad as to make clear that the failure to warn is a basic form of negligence." RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 18 cmt. a (Proposed Final Draft No. 1, 2005) (offering diverse examples). *See also* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(c) (1998) (discussing product liability based on failure to warn); *id.* § 10(a) ("One engaged in the business of selling . . . products is subject to liability for harm . . . caused by the seller's failure to provide a warning after the time of sale . . . if a reasonable person in the seller's position would provide such a warning.").

237. *See* RESTATEMENT (SECOND) OF TORTS § 342 cmt. d (1965) ("[T]he licensee . . . is entitled to expect nothing more than a disclosure of the conditions which he will meet if he . . . enters, in so far as those conditions are known to the giver of the privilege.").

238. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 41 reporter's note to cmt. g (Proposed Final Draft No. 1, 2005) ("Some courts have declined to adopt a duty beyond that of warning. A substantial number of courts, and legislatures enacting statutes, limit the duty to warning the potential victim.").

239. If a court imposes a duty to warn as a matter of common law principles, there are many open questions relating to the method for conveying the warning and the specificity of the message. In the absence of a governing statute, the courts will determine whether the database possessor acted reasonably on a case-by-case basis. However, attorneys advising clients on what they must do to avoid liability might do well to keep in mind that the Interagency Guidance states:

> If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,732 (Mar. 29, 2005) [hereinafter Interagency Guidance].

240. *See id.* at 15,751–53 (setting forth guidance jointly issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, interpreting the GLBA and related provisions). The Interagency Guidance opines that financial institutions have a duty to notify customers of a breach of data security. *See id.* at 15,752 (providing that "[w]here an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator").

> Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance. The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution.[241]

2. The Obligation to Correct Previous Statements

There is a duty to update previous statements that were intended to induce reliance and that, though true when made, have become false or misleading as a result of subsequent developments.[242] The duty extends until recipients of the

---

241. *Id.* at 15,752–53. More specifically, the document provides:

> The notice should include the following additional items, when appropriate:
>
> a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;
>
> b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
>
> c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
>
> d. An explanation of how the customer may obtain a credit report free of charge; and
>
> e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.

Id. at 15,753. The Interagency Guidance adds:

> Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Id. at 15,753.

242. *See* Sharff v. Pioneer Fin. Servs., Inc., No. 92 C 20034, 1993 WL 87718, *6–7 (N.D. Ill Mar. 22, 1993) (recognizing the rule and holding a question of fact existed as to whether the defendant failed to correct a representation that the plaintiff would be given a performance review); Stevens v. Marco, 305 P.2d 669, 683 (Cal. Dist. Ct. App. 1957) (stating that "one who learns that his statements, even if thought to be true when made, have become false through a change in circumstances, has the duty, before his statements are acted upon, to disclose the new conditions to the party relying on his original representations"); St. Joseph Hosp. v. Corbetta Constr. Co., 316 N.E.2d 51, 71 (Ill. App. Ct. 1974) (stating that "where one has made a statement which at that time is true but subsequently acquires new

information are no longer able to protect their own interests by foregoing reliance on the now-erroneous representation of the fact.[243] The purpose of the rule is to avoid deception that causes harm.

McGrath v. Zenith Radio Corp.[244] illustrates the operation of this rule in another context. In that case, the defendants told the plaintiff executive that he was the "heir apparent" to the presidency of a soon-to-be-acquired subsidiary.[245] However, before the plaintiff released his shares of stock and options to facilitate the acquisition, the defendants learned there were serious doubts as to whether the plaintiff would ever become president,[246] but did not disclose those developments to the plaintiff.[247] In an opinion by Chief Judge Thomas E. Fairchild, the Seventh Circuit upheld a judgment in favor of the executive.[248] The court reasoned that, in selling his shares, the plaintiff relied on the defendants' assurances that he would be the new corporate head, and the defendants never advised him to the contrary.[249] "The making of the original statements, the discovery of their falsehood, and the failure to correct them before plaintiff relied on them were 'elements in a continuing course of conduct' capable of establishing fraud."[250]

Similarly, when businesses tell their customers—through advertisements, websites, or published privacy policies[251]—that their personal data is secure, but then learn information to the contrary, the businesses may have a duty to disclose those developments to their customers.[252] The customers have a choice whether to continue their relationships with the businesses in question. There has been no irrevocable reliance by a customer, even though a business-customer relationship

---

information which makes it untrue or misleading, he must disclose such information to anyone whom he knows to be acting on the basis of the original statement—or be guilty of fraud or deceit"); McMahan v. Greenwood, 108 S.W.3d 467, 494 (Tex. App. 2003) (holding that an attorney had a duty "to correct any misimpressions caused by his earlier statements"); 2 FOWLER V. HARPER, FLEMING JAMES, JR. & OSCAR S. GRAY, THE LAW OF TORTS § 7.14, at 476 (2d ed. 1986); *see also* First Nat'l Bank of Elgin v. Nilles, 35 B.R. 409, 411 (N.D. Ill. 1983) ("[O]ne who makes an incorrect statement he has reason to believe another is relying upon is under a duty to correct it.").

243. *See* RESTATEMENT (SECOND) OF TORTS § 551 cmt. h (1977) (providing that "[o]ne who, having made a representation which when made was true or believed to be so, remains silent after he has learned that it is untrue and that the person to whom it is made *is relying* upon it in a transaction with him, is morally and legally in the same position as if he knew that his statement was false when made" (emphasis added)).

244. 651 F.2d 458 (7th Cir. 1981) (applying California law).

245. *Id.* at 462.

246. *Id.* at 462–63.

247. *Id.* at 463.

248. *Id.* at 461.

249. *Id.* at 468.

250. McGrath v. Zenith Radio Corp., 651 F.2d 458, 468 (7th Cir. 1981) (quoting Black v. Shearson, Harrill & Co., 72 Cal. Rptr. 157, 160 (Ct. App. 1968)).

251. *See supra* text accompanying notes 151–55.

252. *Cf.* Thomas J. Smedinghoff, *Trends in the Law of Information Security*, 2 CIPARETI (A.B.A. Chicago, Ill.), Mar. 2005, http://www.abanet.org/buslaw/committees/CL320010pub/newsletter/0006/index.html (stating that "government enforcement agencies such as the Federal Trade Commission (FTC) have actively pursued companies for 'deceptive' trade practices whenever the information security representations they voluntarily make to the public do not match their actual security practices").

is already in progress. The customers may act to protect their interests by terminating the relationship and doing business elsewhere.

Importantly, in *McGrath* and similar cases, the defendants were not guilty of mere negligence, but of fraud. In fraud actions, economic losses are routinely recoverable,[253] except in a minority of states.[254] Consequently, if the law imposes a duty to speak under this theory, the economic-loss rule[255] or the usual requirements of foreseeability may not limit the scope of liability.[256] In addition, "[e]motional harm damages are not ordinarily recoverable in a misrepresentation action,"[257] and thus the issues addressed in Part IV.B may be irrelevant under this theory of liability.

3. Conduct Creating a Continuing Risk of Physical Harm

It is well established that when a person's prior conduct creates a continuing risk of physical harm there is a duty to render assistance to keep the harm from occurring or mitigate adverse consequences.[258] This duty exists even if the prior conduct was not tortious.[259] Thus, a driver who is involved in an auto accident must stop to render assistance, regardless of whether he was at fault for the collision.[260] Likewise, a landlord who sprays an apartment, carelessly or not, with a pesticide

---

253. *See* ROBERT L. DUNN, RECOVERY OF DAMAGES FOR FRAUD 20 (3d ed. 2003) ("[D]ozens of cases are decided every year awarding economic loss damages for fraud."); *id.* at 24–26 (discussing cases that held the economic-loss rule does not apply to misrepresentation claims); *see also id.* at 20 ("If the economic-loss rule is held to bar damages for misrepresentation, the courts are saying that there is no difference between deliberate lying, that is, common-law fraud, and innocent sales of goods that happen not to conform to the contract.").

254. *See id.* at 20 ("[O]nly a minority of states and a few federal courts have held the economic loss rule applicable to fraud claims.").

255. *See infra* Part IV.A.

256. *See* DUNN, *supra* note 253, at 18 ("There is no policy behind limiting the damages recoverable against one who defrauds another to those damages that the party committing the fraud might have been able to foresee at the time he or she made the misrepresentation.").

257. DAN B. DOBBS, THE LAW OF TORTS § 483, at 1381 (2000) [hereinafter TORTS]. *But see* DUNN, *supra* note 253, at 170 ("[C]ourts have divided sharply in recent years as to whether emotional distress is a recoverable element of damages for fraud.").

258. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1, 2005); *see also* RESTATEMENT (SECOND) OF TORTS § 321 (1965) ("(1) If the actor does an act, and subsequently realizes or should realize that it has created an unreasonable risk of causing physical harm to another, he is under a duty to exercise reasonable care to prevent the risk from taking effect. (2) The rule stated in Subsection (1) applies even though at the time of the act the actor has no reason to believe that it will involve such a risk.").

259. *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1, 2005) (creating a duty to render assistance for conduct that creates a continuing risk of harm, "even though not tortious").

260. *Cf.* RESTATEMENT (SECOND) OF TORTS § 321 illus. 3 (1965) (indicating that a driver involved in a accident because his car skids on ice has a duty to warn oncoming drivers).

that makes a tenant ill is obliged, in response to a request, to disclose the pesticide's contents to aid the medical care of the tenant.[261]

The harm caused by intrusions into computerized personal data is typically more economic than physical in nature.[262] Yet, misuse of improperly accessed personal data can result in a physical attack on a data subject or physical harm to property. Hacking of a newspaper's records, for example, may reveal when a customer's paper will be on "vacation hold" and thereby lead to a burglary while the customer is away on vacation.

In *Remsburg v. Docusearch, Inc.*,[263] an Internet-based investigation service obtained a woman's workplace address not through hacking, but by placing a pretext phone call and duping her into revealing her employment information.[264] The party who purchased the data from the service then went to the workplace and killed the woman.[265] The court held that if an "information broker's . . . disclosure of information to a client creates a foreseeable risk of criminal misconduct against a third person whose information was disclosed, the [information broker] owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm."[266] In cases like *Remsburg*, where access to personal data leads to physical harm, hackers may have obtained the personal data from a third party, thus potentially triggering the increased-risk-of-harm rule.

As articulated by the new *Restatement (Third) of Torts*, the existence of a duty of reasonable care under this rule depends upon (1) "prior conduct," that (2) "creates a continuing risk of physical harm," that is (3) "of a type characteristic of the conduct."[267] When someone uses improperly accessed computerized data to cause physical harm, the database possessor's "prior conduct" is the maintenance of the information in a form where one of the foreseeable risks is unauthorized intrusion. That conduct may qualify as tortious (if the database possessor was careless in safeguarding the data) or as innocent (if the database possessor exercised reasonable care or was under no duty). The distinction makes no difference. The loss of the data creates some risk of physical harm to data subjects—often not a great risk, but not a negligible risk either. If the conduct and risk requirements are satisfied, the question is then whether, if physical harm occurs, it is a type of harm "characteristic of the conduct." Concerning this requirement, the *Restatement* commentary offers guidance:

---

261. *See* La Raia v. Superior Court, 722 P.2d 286, 287–90 (Ariz. 1986) ("Having caused or contributed to plaintiff's poisoning, defendant was under a duty to act reasonably to mitigate the resulting harm.").

262. *See* Rustad & Koenig, *supra* note 18, at 93 ("The predominant injury in a cybertort case is a financial loss.").

263. 816 A.2d 1001 (N.H. 2003).

264. *Id.* at 1006.

265. *Id.*

266. *Id.* at 1007.

267. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1, 2005).

> The conduct must . . . be sufficiently connected with the potential for later harm that imposing a duty to prevent or mitigate the harm is appropriate. . . . [I]t is unfair to impose this duty when the actor's conduct has not generally increased the risk of harm . . . or is quite removed from the risks that pose harm to the other . . . .[268]

Whether a defendant's practices in maintaining a database substantially "increased the risk of harm" to the data subject, or are far "removed" from those risks, are matters that depend heavily on the specific facts. In some cases, the connection between the defendant's role in the loss of the information and the resulting threatened physical harm may be sufficiently great to give rise to a duty to warn data subjects about breaches of the security of their personal information. This theory of liability only applies in cases when data subjects suffer physical harm. However, if data subjects suffer personal injuries, the amount of damages may be great.

C. Fiduciary Duty of Candor

A fiduciary relationship imposes a duty of candor. The fiduciary must exercise reasonable care to reveal all material information to the person to whom the fiduciary owes a duty.[269] Indeed, when the interests of the fiduciary and the beneficiary are adversely aligned, fiduciary principles may require something more than reasonable care—perhaps a degree of forthcomingness that approximates "absolute and perfect candor."[270]

If a database possessor owes fiduciary obligations to a data subject (as in the case of an attorney and client), the possessor must disclose information relating to a breach of database security. The interests of the fiduciary and the data subject are in potential conflict because there are important questions as to whether the possessor may be held responsible for the loss of the data. The law requires the fiduciary to subordinate personal interests to the interests of the data subject. Non-disclosure would ordinarily be inconsistent with those heavy obligations.[271]

---

268. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 39 cmt. c (Proposed Final Draft No. 1, 2005).

269. *Cf.* Nicola W. Palmieri, *Good Faith Disclosures Required During Pre-Contractual Negotiations*, 24 SETON HALL L. REV. 70, 127 (1993) (stating that a "party who owes [a] confidential or fiduciary duty has an obligation to divulge or disclose during negotiations all material facts concerning the transaction within his knowledge").

270. *Cf. Candor*, *supra* note 161, at 771 (stating that in legal representation a "duty of 'absolute and perfect candor' applies most forcefully in instances where the interests of the attorney and client are adverse").

271. There are difficult questions as to how far a fiduciary's duty of candor extends. Considerations relating to scope of the relationship, materiality, prior knowledge of the information, competing obligations to others, consent, and likelihood of harm all act to limit the duty. *See Candor*, *supra* note 161, at 778–92. For a discussion of whether a lawyer must tell a client that the lawyer may have committed malpractice, see *id.* at 773 & n.182.

This theory of notification duty, like the earlier discussion of whether fiduciaries have a duty to safeguard computerized personal information,[272] has limited applicability. This theory does not govern the general run of commercial cases. However, this theory may be of great importance in cases involving lawyers, physicians, and other fiduciaries who maintain computerized records containing personal data relating to clients, patients, and beneficiaries.

IV. LIMITING CYBERSECURITY TORT LIABILITY

Assuming that a database possessor breached a duty to protect personal data or to disclose information of unauthorized access to computerized information, how far should tort liability extend? Should an affected data subject be able to recover economic losses or emotional-distress damages that result from the breach? If these or other substantial damages are ordinarily recoverable, is there anything the defendant database possessor can do between the time of the breach and the moment of harm to minimize its exposure to tort liability? The following subparts consider these issues.

A. The Economic-Loss Rule

The economic-loss rule is an "'obscure'"[273] but important legal doctrine, which holds that a plaintiff may not recover economic losses resulting from the defendant's negligence without corresponding physical damage to the plaintiff's person or property.[274] Obviously, if the economic-loss rule applies to cybersecurity cases, it has the potential to greatly limit the scope of recoverable damages.[275] Consequently, it is important to understand the policies underlying the rule and the precise nature of its restrictions. Viewed from the standpoint of public policy, the economic-loss rule serves three very different functions: avoidance of too broad a scope of liability; insistence that damages be proved with certainty; and definition of the doctrinal boundary between contract law and torts.

First, somewhat crudely, the economic-loss rule protects potential defendants from the risk of a disproportionately wide range of liability.[276] This is an important

---

272. *See supra* Part II.D.

273. John J. Laubmeier, Comment, *Demystifying Wisconsin's Economic Loss Doctrine*, 2005 WIS. L. REV. 225, 225–26 ("[T]he application of the doctrine is a constantly developing area of law, which may not be fully understood by judges, lawyers, or the public at large.").

274. *See* Ann O'Brien, Note, *Limited Recovery Rule as a Dam: Preventing a Flood of Litigation for Negligent Infliction of Pure Economic Loss*, 31 ARIZ. L. REV. 959, 959 (1989) ("Under the majority rule, a plaintiff may recover economic losses for negligence only when there is accompanying physical damage to person or property"); *see also* DUNN, *supra* note 253, at 19 ("In the last ten years or so, most courts have held . . . economic loss unaccompanied by property damage or personal injury not to be recoverable in an action alleging negligence or strict liability in the manufacture of a product . . . .").

275. *See* Rustad, *supra* note 3, at 113 ("The economic loss rule adopted by most courts is a barrier to tort recovery for Internet-related security breaches.").

276. *See* JAY M. FEINMAN, ECONOMIC NEGLIGENCE: LIABILITY OF PROFESSIONALS AND BUSINESSES TO THIRD PARTIES FOR ECONOMIC LOSS § 1.2, at 12 (1995) [hereinafter ECONOMIC NEGLIGENCE] (stating that a "distinctive feature of economic negligence cases is the fear of

function, for acts of negligence often have broad adverse economic consequences. Without this protection, there would be no sensible stopping point to tort liability. For example, a referee who negligently made a bad call that eliminated a team from the playoffs could be liable for the lost profits of merchants who sell team-related items,[277] or a person who caused an auto accident could be responsible for all of the economic losses that resulted from the delays of persons tied up in traffic.[278] Not surprisingly, the *Restatement* provides, as a general rule, that there is no liability for negligent interference with contracts or economically promising relations.[279] According to Professor Jay M. Feinman, "[I]ndeterminacy [of the scope of liability in economic negligence cases] is a concern not in and of itself but through its relation to fundamental tort policies. When liability is indeterminate, arguably the deterrence, loss distribution, and fairness policies are undermined."[280]

Second, lost economic opportunities are often not readily susceptible to precise calculation.[281] Yet, the law insists that damages must be proved with reasonable certainty. By ruling out litigation in a huge range of cases (suits involving no personal injury or property damage), the economic-loss rule helps to ensure (again somewhat crudely[282]) that compensation is not awarded for amounts that are

---

indeterminate liability," meaning both the "indeterminacy of the number of potential plaintiffs . . . and the size of their claims"); *id.* § 1.3.2, at 16–19 (discussing the threat of indeterminate liability).

277. *See* Bain v. Gillispie, 357 N.W.2d 47, 49 (Iowa Ct. App. 1984) (holding that injury to novelty store owners' business interests was not a reasonably foreseeable result of a college basketball referee's call that had the effect of eliminating the local team from the conference championship; no liability for "referee malpractice").

278. *Cf.* Kinsman Transit Co. v. City of Buffalo, 388 F.2d 821 (2d Cir. 1968) (denying recovery to persons who incurred additional shipping costs when a bridge collapsed as a result of multiple acts of negligence).

279. *See* RESTATEMENT (SECOND) OF TORTS § 766C (1977) ("One is not liable to another for pecuniary harm not deriving from physical harm to the other, if that harm results from the actor's negligently (a) causing a third person not to perform a contract with the other, or (b) interfering with the other's performance of his contract or making the performance more expensive or burdensome, or (c) interfering with the other's acquiring a contractual relation with a third person."); *see also id.* § 766C cmt. a (opining that courts "apparently have been influenced by . . . the fear of an undue burden upon the defendant's freedom of action, the probable disproportion between the large damages that might be recovered and the extent of the defendant's fault, and perhaps in some cases the difficulty of determining whether the interference has in fact resulted from the negligent conduct").

280. ECONOMIC NEGLIGENCE, *supra* note 276, § 1.3.2, at 18.

281. *Cf.* J'Aire Corp. v. Gregory, 598 P.2d 60, 65 (Cal. 1979) ("The chief dangers . . . in allowing recovery for negligent interference with prospective economic advantage are the possibility of excessive liability, the creation of an undue burden on freedom of action, the possibility of fraudulent or collusive claims and the *often speculative nature of damages*." (emphasis added)).

282. This is not the only occasion when the law employs a rather blunt rule to limit the scope of tort liability. In some states, for example, there is no liability for negligent infliction of emotional distress unless the plaintiff suffers some form of physical impact or physical consequences. *See* Brown v. Matthews Mortuary, Inc., 801 P.2d 37, 45 (Idaho 1990) (holding that, absent physical manifestations of injury, a son could not recover for distress allegedly resulting from mortuary's negligent loss of the cremated remains of his father); Bader v. Johnson, 732 N.E.2d 1212, 1221–22 (Ind. 2000) (indicating that Indiana continues to adhere to a modified impact rule).

speculative.[283] In the process, the economic-loss rule promotes judicious use of limited judicial resources, ensuring that those scarce assets are not squandered on the burdensome, and perhaps dubious, task of trying to quantify endless economic losses that may, in truth, not be provable with reasonable precision.[284]

Third, and most importantly, the economic-loss rule marks the boundary-line between contract law and tort law.[285] Delineating these two bodies of law is vital, for otherwise there is a risk that "contract law would drown in a sea of tort."[286] The law of contracts has meaning only because entering into an agreement has legal consequences. One of those consequences is that if a person makes a bad deal, he usually must suffer the result. This reality creates an incentive for contracting parties to exercise diligence to protect their own interests.[287] It would render superfluous a great part of contract law if parties who strike disadvantageous bargains could successfully complain that they should recover damages because the other side failed to exercise reasonable care to protect their interests.

The best example of how the economic-loss rule distinguishes contract claims from torts is *East River Steamship Corp. v. Transamerica Delaval*,[288] a case involving a defective product. That suit, which eventually reached the nation's

---

283. *But see* DUNN, *supra* note 253, at 18–19 ("The rule that precludes recovery of uncertain and speculative damages applies where the *fact* of damages is uncertain, not where the *amount* is uncertain. . . . Computation of the amount is for the trier of fact.").

284. *See* JOHNSON & GUNN, *supra* note 38, at 7, 9 ("It has often been urged that . . . . [t]ort law should be administratively convenient and efficient, and should avoid intractable inquiries. Only a limited amount of resources can be devoted to the administration of justice in any society. This principle holds that tort rules should be shaped so that the dollars spent on accident compensation are efficiently employed. Thus, legal standards should not be so complex or uncertain that their application entails an undue expenditure of judicial resources or imposes unnecessarily high litigation costs on parties. So, too, convenience and efficiency discourage the pursuit of what might be called intractable inquiries, matters where the facts are such that even after expenditure of considerable time and money, there is a substantial risk that an erroneous result will be reached.").

285. *See Doctrinal Classification*, *supra* note 34; *see also* Daanen & Janssen, Inc. v. Cedarapids, Inc., 573 N.W.2d 842, 846 (1998) ("Application of the economic loss doctrine to tort actions between commercial parties is generally based on three policies, none of which is affected by the presence or absence of privity between the parties: (1) to maintain the fundamental distinction between tort law and contract law; (2) to protect commercial parties' freedom to allocate economic risk by contract; and (3) to encourage the party best situated to assess the risk [of] economic loss, the commercial purchaser, to assume, allocate, or insure against that risk."); ECONOMIC NEGLIGENCE, *supra* note 276, § 1.3.3, at 20–21 (discussing the protection of private ordering).

286. E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 866 (1986); *see generally* Vincent R. Johnson, *Liberating Progress and the Free Market from the Specter of Tort Liability*, 83 NW. U. L. REV. 1026, 1030 (1989) [hereinafter *Liberating Progress*] (stating that, according to one legal commentator, "ever-more-generous incarnations of tort law ascended to the throne of accident compensation following the decline of privity, the narrowing construction of disclaimers, and the widely heralded 'death of contract'" (citing GRANT GILMORE, THE DEATH OF CONTRACT (1974))).

287. *See* JOHNSON & GUNN, *supra* note 38, at 9 (noting that it has often been urged that the law should be shaped to "promote individual responsibility" and to encourage persons "to employ available resources to protect their own interests, rather than depend upon others to save them from harm" (emphasis omitted)).

288. 476 U.S. 858 (1986); *see also* Glaub Jewelers, Inc. v. New York Daily News, 535 N.Y.S.2d 532, 534 (Civ. Ct. 1988) (holding that a newspaper that negligently failed to publish an advertisement for a business was not liable in tort for the business's lost sales).

highest court, involved a defective component part of a turbine that damaged only the turbine itself.[289] There was no harm to any person or to the plaintiff's "other" property.[290] The action sought damages in tort for the cost of repairs to the turbine and for lost profits because statutes of limitations already barred the plaintiff's contract claims.[291] The Supreme Court, in an opinion by Justice Harry Blackmun, held that a manufacturer has no tort duty under negligence or strict liability to prevent a product from injuring itself.[292] Those types of harm are merely economic losses that parties can insure against or otherwise address while negotiating the contract.[293] Only product defects that result in harm to property other than the product itself or in personal injury are cognizable under the law of torts.[294] The law of warranty provides sufficient protection for the benefits of the bargain.[295]

With these three policy considerations in mind—scope of liability, certainty of damages, and delineation of contract-versus-tort—the question is then whether the economic-loss rule should apply to cybersecurity cases and, if so, what claims for damages the rule might bar. Answering those questions involves consideration of the types of economic losses that may arise in these cases, as well as the efficacy of contract law and the insurance market in addressing such losses. Unauthorized use of personal information can result in many types of harm. In cybersecurity cases where breaches of security result in identity theft, the losses include, but are not limited to: (1) out-of-pocket expenses incurred to restore a good credit rating; (2) personal time spent on that task; and (3) lost opportunities resulting from bad credit.

Focusing first on out-of-pocket losses,[296] there is little policy justification for denying recovery. Various estimates currently peg out-of-pocket costs in a typical case between $800[297] and $1,400.[298] Although the amount of out-of-pocket damages may vary from case to case, this element of damages is susceptible to proof with a

---

289. *E. River S.S. Corp.*, 476 U.S. at 860–61.

290. *Id.*

291. *Id.* at 861.

292. *Id.* at 870.

293. *Id.*

294. E. River S.S. Corp. v. Transamerica Delaval Inc., 476 U.S. 858, 871–72 (1986).

295. *Id.* at 873.

296. Presumably these costs would include items such as postage, phone calls, photocopying, gasoline, and the like, as well as the cost of obtaining court documentation that one is the victim of identity theft. Out-of-pocket costs may also include payments attributable to increased interest charges on legitimate credit card expenditures that are assessed because the identity theft victim has a bad credit rating. *See* Zeller, *supra* note 4, at C1 (stating, with regard to one identity theft victim, that "because his credit rating had been severely damaged, the interest rates on some of Mr. Fairchild's legitimate cards began climbing, while the credit limits he had been extended on his cards suddenly began to drop—even though his payments were on time"). Moreover, a financial institution or other entity may sue the identity theft victim for a debt incurred by the identity theft perpetrator, and the victim may need to spend money out of pocket to defend against those charges. *See id.* (describing an instance when "one of many institutions that had bought and sold" a wrongfully incurred mortgage debt sued a victim of identity theft who therefore "required the help of a lawyer").

297. *See Stop Thieves*, *supra* note 1, at 12 (stating that victims of identity theft "typically lose $800 and spend two years clearing their names").

298. SENATE COMM. ON CRIMINAL JUSTICE, BILL ANALYSIS, Tex. C.S.S.B. 122, 79th Leg. R.S. (2005), *available at* Tx. B. An., S.B. 122, 4/7/2005 (Westlaw).

high degree of certainty. The plaintiff can gather receipts, make a list, and total the sum. There is no reason to deny compensation for amounts actually and reasonably spent on restoring a good credit rating on the ground that out-of-pocket damages are speculative.

Nor does recovery of out-of-pocket costs present a case that requires a tightly circumscribed circle of liability to prevent an over extension of legal responsibility. In many cases, there will be a business relationship between the database possessor and the damaged data subject, and in other cases the relationship (presumably) is sufficiently close enough that the defendant had some legitimate reason to maintain a database containing personal information about the plaintiff.[299] These are not situations where some "stranger" in the community (e.g., the vendor of the losing team's products[300] or the person tied up in traffic[301]) is seeking to recover damages. If a database possessor wishes to constrict the scope of potential liability, it can always do so by removing the personal information of data subjects from its database. But if it fails to do so, courts should be reluctant to deny recovery of out-of-pocket losses to data subjects. The database possessor chose to maintain personal information in a form where one of the risks was unauthorized access.

If the scope of liability and uncertainty of damages are not significant considerations, the only question, so far as the economic-loss rule is concerned, is whether the boundary-line between contracts and torts creates a good reason for a court to say this is the type of loss that should be compensated only if a contractual obligation exists. The answer to that question is no.

An emerging consensus, reflected in the recently passed state security breach notification statutes, suggests that rights relating to protection of personal data and notification of security breaches *are not* proper subjects for bargaining between the parties. Many state laws, such as the Rhode Island Identity Theft Protection Act of 2005,[302] provide that a waiver of the data subjects' rights is against public policy, and therefore void and unenforceable.[303] If that is true, it makes little sense that consumers should bargain and pay for the level of cybersecurity protection—and the right to sue for out-of-pocket damages—that they desire. Moreover, it is simply unrealistic to expect that bargaining to occur between individual consumers and the large corporations that play a pervasive role in modern life. Individuals often lack

---

299. Indeed, if the database possessor had no legitimate reason for maintaining the personal information of the data subject, a court may not relieve the possessor of exposure to liability.

300. *See supra* note 277 and accompanying text.

301. *See supra* note 278 and accompanying text.

302. Rhode Island Identity Theft Protection Act of 2005, ch. 225, sec. 1, § 11-49.2-6(B), 2005 R.I. Gen. Laws Adv. Legis. Serv. (LexisNexis), *available at* 2005 R.I. ALS 225 (LexisNexis).

303. *See* Personal Information Protection Act, ch. 110, § 4-110-107, 2005 Ark. Legis. Serv. (West), *available at* AR LEGIS 1526 (2005) (Westlaw) ("Any waiver of a provision of this subchapter is contrary to public policy, void, and unenforceable."); CAL. CIV. CODE § 1798.84(a) (West Supp. 2005); Personal Information Protection Act, Pub. Act 94-36, ch. 815, sec. 530, § 15, 2005 Ill. Legis. Serv. (West), *available at* IL LEGIS 94-36 (2005) (Westlaw); Act of June 2, 2005, ch. 167, sec. 1, § 3, 2005 Minn. Sess. Law Serv. (West), *available at* MN LEGIS 167 (2005) (Westlaw); Act of June 17, 2005, ch. 486, sec.17, § 27, 2005 Nev. Stat., *available at* NV LEGIS 486 (Westlaw); Act of May 10, 2005, ch. 368, § 9, 2005 Wash. Legis. Serv. (West), *available at* WA LEGIS 368 (2005) (Westlaw).

both the commercial leverage[304] and the information necessary to assess the risks they face. "[I]t would be entirely possible that despite good faith efforts and the expenditure of considerable funds, a customer would fail to obtain a fully accurate and complete picture of potential harms, with the result being an unintentional and undesired assumption of risk by the consumer."[305] In light of the ubiquity of computerized databases, ordinary persons would have to devote a huge amount of energy to negotiating the parameters of data protection with every potential defendant if contract law were the only solution to these types of problems. As a result, "[c]onsumers would spend an inordinate amount of resources on efforts to perform often duplicative, time-consuming tasks relating to assessment of the risks of injury and the need for economic protection."[306]

As an alternative to this sort of David-versus-an-army-of-Goliaths contractual model, a better paradigm would routinely permit recovery of foreseeable and necessary out-of-pocket losses from the tortfeasor. Compensation of out-of-pocket losses should not depend upon whether the data subject read the fine print in the defendant's privacy policy or bargained for a specific level of protection. Instead, compensation should depend on the reasonableness of the amount spent to restore a good credit rating. Tort law can perform this function better than contract law.[307] Moreover, the function is not one for which the insurance market has offered an adequate substitute. According to *Consumer Reports*, "ID theft insurance is typically not worth paying for."[308]

The preceding analysis of the propriety of awarding out-of-pocket credit-repair damages can be profitably contrasted with requests for recovery and compensation for time spent restoring one's good credit or for opportunities lost as a result of a bad credit rating. Victims of identity theft spend six hundred hours on average to restore their credit.[309] The harm suffered by these victims is tremendous, but valuing these lost hours would be difficult. If these damages amounted to compensation for the plaintiffs' time measured at their usual hourly rate of earnings, the awards to professionals, minimum wage workers, and unemployed

---

304. *See Liberating Progress*, *supra* note 286, at 1044 (discussing the "the inequalities of bargaining power which pervade many consumer transactions" and noting that "[p]urveyors of goods and services frequently employ standardized contracts which leave consumers little choice but to accept a deal as presented—including contractual terms which purport to limit the provider's liability to the consumer").

305. *Id.* at 1042.

306. *Id.*

307. In contract law, consequential damages are not recoverable unless they were specifically in the mind of the parties at the time the parties entered into the contract. *See* DAN B. DOBBS, LAW OF REMEDIES §§ 12.4(4)–4(6), at 779–89 (2d ed. 1993) (discussing the "contemplation of the parties rule"). Consequently, it would be difficult to recover out-of-pocket credit-repair damages under a contractual theory of liability.

308. *Stop Thieves*, *supra* note 1, at 12. "Policies generally cover the expenses of cleaning up the crime, including attorney's fees, costs of mailing correspondence, and lost wages. They seldom cover the out-of-pocket loss to the victim . . . ." *Id.* at 14.

309. *See* SENATE COMM. ON CRIMINAL JUSTICE, BILL ANALYSIS, Tex. C.S.S.B. 122, 79 th Leg. R.S. (2005), *available at* Tx. B. An., S.B. 122, 4/7/2005 (Westlaw). *But see* McMahon, *supra* note 4, at 626 n.5 ("average victim spends 175 hours to clear name" (citing 147 CONG. REC. S12162 (daily ed. Nov. 29, 2001) (statement of Ms. Cantwell))).

homemakers would vary widely—perhaps without good reason. Similarly, if every victim received the same amount for the value of lost time, how would that amount be set? Ensuring uniformity in valuing damages for lost time is a task better committed to legislatures than to the multitude of fact-finders who will preside over numerous tort claims.

The problems of compensating for the value of lost opportunities—such as the lost chance to buy a house, obtain a car loan, or open a cell phone account—are also obvious. How does one prove precisely which opportunities the plaintiff lost and what those opportunities meant in economic terms to the plaintiff? In addition, there is a clear risk of imposing an excessively wide range of liability. Negligence requires only a momentary misstep, whether in the data protection arena or in other contexts. To say that a negligent database possessor should be liable to a broad class of persons for all of their lost opportunities—as well as out-of-pocket and perhaps other damages—would quickly pose a serious risk of liability disproportionate to fault.[310] These issues suggest that courts have a greater reason to apply the economic-loss rule to bar claims for lost time and lost opportunities than to hold that a plaintiff cannot recover out-of-pocket losses.

The economic-loss rule, as defined in most states, has important limits. First, it bars only claims for economic harm caused bv negligence.[311] A plaintiff may thus be able to avoid the rule by proving more culpable conduct, such as recklessness or intentional wrong-doing.[312] Second, the economic-loss rule is a common law

---

310. *See* JOHNSON & GUNN, *supra* note 38, at 7 ("The proportionality principle seeks to limit or refine application of the fault principle. In part, it holds that liability should not be levied on an individual tortfeasor, even if fault is shown, if doing so would expose the defendant to a burden that is disproportionately heavy or perhaps unlimited."). The proportionality principle is one of the most important forces in modern American tort law. To avoid imposition of disproportionate liability, courts and legislatures have crafted limited-duty rules, *see* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 41 reporters' note to cmt. g (Proposed Final Draft No. 1, 2005) (discussing the sometimes-limited duties of mental-health professionals); imposed what amount to "standing to sue" requirements, *see* Kinard v. Augusta Sash & Door Co., 286 S.C. 579, 583, 336 S.E.2d 465, 467 (1985), (stating that in bystander cases seeking recovery for negligent infliction of emotional distress "the plaintiff and the victim must be closely related"); restricted the types of damages that are recoverable, *see* Rieck v. Medical Protective Co. of Fort Wayne, Ind., 219 N.W.2d 242, 249–45 (Wis. 1974) (denying recovery of child-rearing costs in failure-to-diagnose-pregnancy cases because that element of damages would be "wholly out of proportion to the culpability involved"); embraced comparative responsibility defenses, *see* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 25 (Proposed Final Draft No. 1, 2005) (discussing the defense in strict liability cases); and limited recovery of damages to harm proximately caused, *see* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM ch. 6 (Proposed Final Draft No. 1, 2005) (discussing the scope of liability).

311. *Cf.* People v. Ware, No. H025167, 2003 WL 22120898, *1–2 (Cal. Ct. App. Sept. 11, 2003) (affirming an award of restitutionary damages, including an amount for the value of business hours the victim spent repairing her damaged credit, because the legislature intended "'that a victim of crime who incurs any economic loss as a result of the commission of a crime shall receive restitution directly from any defendant convicted of that crime'") (quoting CAL. PENAL CODE § 1202.4(a)(1) (West 1995) (amended 2004)).

312. "In the absence of physical damage, tort recovery for pure economic loss is limited to 'wilful' infliction of economic loss." O'Brien, *supra* note 274, at 959–60 (quoting W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON & DAVID G. OWEN, PROSSER AND KEETON ON THE LAW OF TORTS § 129, at 1000 (5th ed. 1984)).

doctrine that does not preempt legislative provisions to the contrary. Liability for negligently caused economic harm may be actionable pursuant to statute. At least one state, Illinois, expressly allows for recovery of economic losses in cybersecurity cases.[313] Third, many types of harm caused by intrusion are not purely economic. Thus, the rule does not bar recovery of damages for personal injury, property damage, and, perhaps, emotional distress. Fourth, some states show little enthusiasm for the economic-loss rule[314] and may determine that it does not apply to cybersecurity cases. Finally, virtually all states that embrace the economic-loss rule recognize some exceptions.[315] For example, economic damages are routinely recoverable in negligent misrepresentation actions.[316] Many states allow persons whose legacies are lost due to negligent preparation of a will to sue to recover those economic damages.[317] A court might determine the relationship between a database possessor and data subject is sufficiently "special"[318] to warrant recovery of out-of-pocket losses resulting from identity theft—notwithstanding the economic-loss rule.

B. Emotional-Distress Damages

States differ tremendously over whether negligently caused emotional-distress claims are actionable.[319] Some jurisdictions hold that emotional-distress damages

313. *See supra* note 195 and accompanying text.

314. *See* ECONOMIC NEGLIGENCE, *supra* note 276, § 1.2, at 11 (1995) ("The traditional view is that personal injury is qualitatively different from economic loss because the former often has catastrophic consequences for the victim and because monetary compensation is unable to wholly remedy injury of this kind; therefore, negligence principles should be confined to cases of personal injury. This view is now controversial; it has been challenged by the many courts that have applied ordinary negligence principles to cases of economic loss . . . ."); CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 50 ("Many courts . . . are beginning to reject the economic loss doctrine. For example, in *People Express Airline v. Consolidated Rail Corporation*, the New Jersey Supreme Court concluded that 'a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty.'" (quoting People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 118 (N.J. 1985)).

315. *See, e.g.*, Laubmeier, *supra* note 273, at 235–43 (discussing exceptions to the economic-loss rule in Wisconsin).

316. *See* RESTATEMENT (SECOND) OF TORTS § 552B cmt. a (1977) (allowing recovery of out-of-pocket losses resulting from negligent misrepresentation).

317. *See, e.g.*, Heyer v. Flaig, 449 P.2d 161, 163 (Cal. 1969) ("An attorney who negligently fails to fulfill a client's testamentary directions incurs liability in tort for violating a duty of care owed directly to the intended beneficiaries." (emphasis added)), *overruled on other grounds by* Laird v. Blacker, 828 P.2d 691, 698 (Cal. 1992).

318. J'Aire Corp. v. Gregory, 598 P.2d 60, 63 (Cal. 1979) ("Where a special relationship exists between the parties, a plaintiff may recover for loss of expected economic advantage through the negligent performance of a contract although the parties were not in contractual privity.").

319. *See* JOHNSON & GUNN, *supra* note 38, at 577 ("No area of tort law is more unsettled than compensation for negligent infliction of emotional distress. The decisions continually restate the criteria for recovery, and there are often substantial differences in the requirements, or their interpretation, from one jurisdiction to the next, and within any one jurisdiction at different times.").

are almost never recoverable,[320] but others seem quite willing to entertain claims for psychic suffering caused by a tortfeasor's failure to exercise due care.

One arena in which a consensus of sorts has emerged is the fear-of-disease cases.[321] In these suits, the plaintiff alleges that the defendant's tortious conduct subjected the plaintiff to emotional distress based on fear of contracting a contagious disease. Many of these cases have involved fear of contracting HIV or AIDS, but the precedent extends somewhat further to fear of cancer and other diseases.

In addressing these claims, courts generally hold that a plaintiff may only recover emotional-distress damages if the plaintiff was actually exposed to the disease.[322] Courts deem fear of disease in the absence of exposure to be unreasonable and therefore not compensable.[323]

However:

> [T]he critical question is whether "exposed" means (a) that the defendant had the disease [when he or she came into contact with the plaintiff], (b) that the circumstances were such that the disease might have been transmitted, (c) that it is probable that the plaintiff will develop the disease, or (d) that the plaintiff in fact contracted the disease.[324]

---

320. *Cf.* Charles E. Cantu, *An Essay on the Tort of Negligent Infliction of Emotional Distress in Texas: Stop Saying It Does Not Exist*, 33 ST. MARY'S L.J. 455, 465–68 (2002) (discussing the Texas Supreme Court's retreat from a broad interpretation of the tort).

321. *See generally* Kimberly C. Simmons, Annotation, *Recovery for Emotional Distress Based on Fear of Contracting HIV or AIDS*, 59 A.L.R. 5th 535, 549 (1998) ("Most often crucial to the success of a claim is whether the particular jurisdiction or court required proof of actual exposure to a disease-causing agent . . . .").

322. *See* Majca v. Beekil, 701 N.E.2d 1084, 1090 (Ill. 1998) (holding that a complaint, alleging that a dental student was infected with HIV at time he provided treatment to the plaintiffs, failed to state a cause of action for fear of contracting AIDS absent proof that the patients were actually exposed to HIV); K.A.C. v. Benson, 527 N.W.2d 553, 557 (Minn. 1995) (holding that a patient, who did not allege that she was actually exposed to HIV, was not in the zone of danger and could not recover for negligent infliction of emotional distress); *see also* Brzoska v. Olson, 668 A.2d 1355, 1357 (Del. 1995) (holding that "there can be no recovery for fear of contracting a disease in the absence of a showing that any of the plaintiffs had suffered physical harm"). *But see* Temple-Inland Forest Prods. Corp. v. Carter, 993 S.W.2d 88, 91 (Tex. 1999) (holding that workers who were exposed to asbestos, but who did not currently have an asbestos-related disease, could not recover damages for fear of developing such a disease in the future).

323. *See supra* note 322 and accompanying text. *But see* Madrid v. Lincoln County Med. Ctr., 923 P.2d 1154, 1159 (N.M. 1996) (permitting recovery without actual exposure where the plaintiff came into contact with bodily fluids that might have been, but were not, HIV-positive).

324. JOHNSON & GUNN, *supra* note 38, at 579.

Courts have answered this question differently,[325] yet the precedent that has emerged in these cases provides a logical starting point for determining whether a data subject should be able to recover for emotional-distress losses resulting from unauthorized database intrusion and fear of identity theft or other harm. If there is no evidence that an intruder actually accessed the plaintiff's data, and the evidence proves only a risk of unauthorized access,[326] courts ordinarily should deny emotional-distress damages, which are inherently difficult to quantify. For example, in one case the evidence showed that "hackers appeared to have been more interested in using . . . [a university's] computer to download movies and music than to access personal data."[327]

In proving that the plaintiff's personal data was subject to unauthorized access, courts reasonably may employ a presumption of unauthorized access. If the defendant has allowed or caused the best evidence of exposure to be lost or destroyed, courts reasonably may assume that exposure occurred absent proof to the contrary. Some fear-of-disease cases take this approach.[328]

In cases involving *intentional* infliction of emotional distress, courts have assiduously required that the distress be severe before it is compensable.[329] This severity requirement is all the more applicable to cases where distress results from mere alleged negligence. Presumably, in only rare cases will it be possible for a data subject who does not suffer physical harm to recover emotional-distress damages relating to data intrusion.

C. Security-Monitoring Damages

Database possessors who suffer a security breach are often reluctant to discover and report those developments[330] for fear of triggering adverse publicity, legal

---

325. *Compare* Johnson v. W. Va. Univ. Hosps., Inc., 413 S.E.2d 889, 893–94 (W. Va. 1991) (permitting recovery where the defendant hospital negligently failed to advise a security officer that an unruly patient had AIDS, and the patient bit the officer after biting himself), *with* Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 800 (Cal. 1993) (holding that "recovery of damages for fear of cancer in a negligence action should be allowed only if . . . the fear stems from a knowledge, corroborated by reliable medical and scientific opinion, that it is more likely than not that the feared cancer will develop in the future due to the toxic exposure").

326. *See* Henry K. Lee, *Bay Area; Trail of Stolen Laptop Winds through Web: Computer Had Data for UC Berkeley Students, Alumni*, S.F. CHRON., Sept. 16, 2005, at B1 (discussing recovery of a stolen laptop where there was "no evidence of identity theft").

327. Ensslin, *supra* note 13, at 22A (explaining that the hackers had access to information about 42,900 persons).

328. *See* S. Cent. Reg'l Med. Ctr. v. Pickering, 749 So. 2d 95, 102 (Miss. 1999) (holding that if "the defendant allowed or caused the best evidence [of exposure to HIV or another communicable disease] to be destroyed, despite the fact that the defendant had notice that a material, factual issue existed regarding that evidence, . . . a rebuttable presumption of actual exposure would arise in favor of the plaintiff").

329. *See, e.g.*, Russo v. White, 400 S.E.2d 160, 163 (Va. 1991) (allowing recovery only where "distress . . . is so severe that no reasonable person could be expected to endure it").

330. *See* Preston & Turner, *supra* note 26, at 459–60 ("Underreporting computer security incidents is not limited to the U.S.—one European study estimates 30,000 to 40,000 occurred in one European nation, while only 105 official complaints were made." (citing COMM'N OF THE EUROPEAN

liability,[331] or increased attacks by hackers.[332] As a result, there is often an undesirable lag between the occurrence of an intrusion, discovery of that breach, and revelation of the events to data subjects.[333] Indeed, sometimes database possessors never tell data subjects about the breach.[334] Yet, as noted above,[335] revelation that a breach of security occurred enables data subjects to protect their interests through increased vigilance against identity theft and other types of harm.[336]

Notification can also be consistent with a database possessor's own interests. Timely notice to customers may protect a company's reputation, reduce its risk of legal liability, and minimize the chances of customer defections.[337] "Requiring businesses to disclose information security violations [also] provides operators with a market incentive to ensure that their security is adequate."[338]

State security breach notification laws currently provide only a limited incentive for database possessors to discover intrusion because legislatures ordinarily base notification obligations on actual discovery or notification of the intrusion rather than when the database possessor should have discovered the breach.[339] In addition, legislatures typically impose a low cap on the civil fines that

---

CMTY., PROPOSAL FOR A COUNCIL FRAMEWORK DECISIONS ON ATTACKS AGAINST INFORMATION SYSTEMS 5 (2002))); Wible, *supra* note 16, at 1612 n.170 (stating that reluctance to report security vulnerability in part reflects "a lack of faith in law enforcement").

331. *See* Marc S. Friedman & Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway*, 9 J. PROPRIETARY RTS. 2, 2 (1997) ("[O]rganizations often swallow losses quietly rather than notifying the authorities and advertising their vulnerability to shareholders and clients.").

332. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 35 ("[I]nformation in the public domain about the vulnerability of a network could lead to copycat attacks."); Wible, *supra* note 16, at 1578 n.6 (asserting that some companies fear that disclosure "both invites retributive attacks and highlights vulnerabilities to other hackers").

333. *See* SENATE RULES COMM., BILL ANALYSIS, Cal. A.B. 700, 2001-2002 R.S. (2002), *available at* CA B. An., A.B. 700 Sen., 8/22/2002 (Westlaw) (discussing hearings "to explore why the breach, which reportedly occurred on April 5, 2002, was not discovered until May 7, 2002 and employees were not notified until May 21, 2002").

334. *See id.* (discussing a case where "a former employee sold hundreds of financial records to an identity theft ring but the company never told its customers").

335. *See supra* note 229 and accompanying text.

336. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 59 ("Disclosure is a common vehicle for consumer protection . . . ."); Preston & Turner, *supra* note 26, at 460 ("[W]hen consumers have notice of unauthorized access to their personal information, they can take steps to mitigate the potential harm by informing credit reporting agencies and responding to fraudulent attempts to exploit their good names.").

337. Interagency Guidance, *supra* note 239, at 15,752.

338. Preston & Turner, *supra* note 26, at 460.

339. *See, e.g.*, Database Security Breach Notification Law, ch. 51, § 3074(A), 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw) (mandating that a database possessor "shall, following discovery of a breach . . . notify"); Identity Theft Enforcement and Protection Act, ch. 294, sec. 2, § 48.103(b), 2005 Tex. Sess. Law Serv. (West), *available at* 2005 TX LEGIS 294 (2005) (Westlaw) (providing that businesses "shall disclose any breach . . . after discovering or receiving notification of the breach").

apply to a breach of a general statutory duty to protect customer information, which may provide insufficient inducement for best practices.[340]

Because "[v]ictims of identity theft must act quickly to minimize . . . damage" and "expeditious notification of possible misuse of a person's personal information is imperative,"[341] legislatures should give database possessors a legal incentive to discover and report unauthorized database intrusions. That incentive could take the form of a limitation on liability. One reasonable option would be to cap the database possessor's exposure to liability at the moment the database possessor reveals the breach to the data subject.[342] Notification could serve as the pivotal factor in shifting further responsibility (beyond the damages cap) from the database possessor to the data subject. Once the database possessor provides notice of the security breach, the data subject is in a better position than the database possessor to monitor the risk of harm and to take action against threats to the data subject's credit and personal security.

The cap on damages could take the form of limiting liability to an amount equivalent to the out-of-pocket costs of monitoring security and taking reasonably necessary steps to prevent identity theft and other losses. These "security-monitoring damages" would be similar in concept to the medical monitoring damages that some state[343] and federal[344] courts allow victims of toxic exposure to

---

340. *See, e.g.*, Identity Theft Enforcement and Protection Act, ch. 294, sec. 2, §§ 48.201(a), (e), 2005 Tex. Sess. Law Serv. (West), *available at* 2005 TX LEGIS 294 (2005) (Westlaw) (holding violators "liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation" and allowing the attorney general to recover "reasonable expenses . . . including reasonable attorney's fees, court costs, and investigatory costs").

341. Database Security Breach Notification Law, ch. 51, § 3072, 2005 La. Sess. Law Serv. (West), *available at* LA LEGIS 499 (2005) (Westlaw).

342. The database possessor should have the duty of proving that the data subject was notified of the breach or that the possessor did everything reasonable to provide notice. This is especially true when aggregate forms of communication are used to disclose security breaches to a large class of persons.

343. *See, e.g.*, Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824–25 (Cal. 1993) ("[T]he cost of medical monitoring is a compensable item of damages where . . . the need for future monitoring is a reasonably certain consequence of a plaintiff's toxic exposure and . . . the recommended monitoring is reasonable. In determining the reasonableness and necessity of monitoring, the following factors are relevant: (1) the significance and extent of the plaintiff's exposure to chemicals; (2) the toxicity of the chemicals; (3) the relative increase in the chance of onset of disease in the exposed plaintiff as a result of the exposure, when compared to (a) the plaintiff's chances of developing the disease had he or she not been exposed, and (b) the chances of the members of the public at large of developing the disease; (4) the seriousness of the disease for which the plaintiff is at risk; and (5) the clinical value of early detection and diagnosis."); Askey v. Occidental Chem. Corp., 477 N.Y.S.2d 242, 247 (N.Y. App. Div. 1984) (allowing recovery of medical monitoring damages to "permit the early detection and treatment of maladies [because] as a matter of public policy the tort-feasor should bear its cost"); Redland Soccer Club, Inc. v. Dep't of the Army, 696 A.2d 137, 145 (Pa. 1997) (finding "no reason to limit common law medical monitoring claims to asbestos-related injuries"); Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 429–31 (W. Va. 1999) (recognizing that a "cause of action exists . . . for the recovery of medical monitoring costs"). *But see* Henry v. Dow Chem. Co., 701 N.W.2d 685, 689 (Mich. 2005) (holding that medical monitoring was not a cognizable negligence claim absent physical injury); Badillo v. Am. Brands, Inc., 16 P.3d 435, 441 (Nev. 2001) ("Nevada common law does not recognize a cause of action for medical monitoring. A remedy of medical monitoring may be available for an underlying cause of action but neither party . . . briefed the issue nor set forth the cause of action to which it would

recover. The analogy is apt, as at least one court has found.[345] A data subject who loses personal data due to a security breach, like a person who suffers exposure to a toxic substance, is at risk of further harm.[346] The harm (e.g., identity theft in the case of the data subject or cancer in the case of the toxic-exposure victim) may or may not later occur.[347] However, the reasonable and prudent course is to incur the expenses necessary to monitor the risk that harm may develop. The victim of the exposure is thereby in a better position to take prompt action—in one case, to combat the risk of financial harm and other risks from data misuse, and in the other, to secure medical care to address the risk of developing an illness.

The concept of shifting responsibility is not new to the law.[348] Some cases hold that a party who creates a risk is not a proximate cause of harm that later occurs.[349]

---

provide a remedy."); Theer v. Philip Carey Co., 628 A.2d 724, 733 (N.J. 1993) (holding that an asbestos worker's wife, who was indirectly exposed to the product, could not recover medical surveillance damages).

344. *See, e.g.*, Carey v. Kerr-McGee Chem. Corp., 999 F. Supp. 1109, 1119 (N.D. Ill. 1998) (predicting that "the Illinois Supreme Court would uphold a claim for medical monitoring"); Witherspoon v. Philip Morris, Inc., 964 F. Supp. 455, 467 (D.D.C. 1997) (recognizing medical monitoring damages under District of Columbia law, but finding that the plaintiff failed to prove "present injury and a reasonable fear that the present injury could lead to the future occurrence of disease"); *see also* MARTIN A. KOTLER, PRODUCTS LIABILITY AND BASIC TORT LAW 328 (2005) (stating that the issue has been "considered by a significant number of state courts and federal courts applying or predicting state law and, while it is generally recognized that monitoring expenses are a recoverable item of damages if an actionable tort is established, many courts have concluded that they are not otherwise recoverable as an independent claim").

345. *See* Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185PHXSRB, 2005 WL 2465906, at *3 (D. Ariz. Sept. 6, 2005) ("The Court is not convinced that the negligent exposure of confidential personal information is entirely dissimilar from negligence exposure to toxic substances or unsafe products."); *see also* People v. Ware, No. H025167, 2003 WL 22120898, *2 (Cal. Ct. App. Sept. 11, 2003) (affirming an award of restitutionary damages to a victim of identity theft, including "$100 per year for monitoring the adverse consequences on her credit rating").

346. *Stollenwerk*, 2005 WL 2465906, at *3.

347. *Id.*

348. *See generally* RESTATEMENT (SECOND) OF TORTS § 452 cmt. f (1965) (discussing the shifting of responsibility to a third person).

349. In some cases, a contractual or statutory allocation of responsibilities between multiple parties is important. *See* Goar v. Vill. of Stephen, 196 N.W. 171, 174 (Minn. 1923) (holding that the duty to prevent harm shifted from a power company that negligently installed electrical lines to a village that negligently inspected and maintained the lines, because the village had contractually assumed those obligations); First Assembly of God, Inc. v. Tex. Utils. Elec. Co., 52 S.W.3d 482, 492 (Tex. App. 2001) (holding that where a statutory tariff provided that "the church 'assumes full responsibility for electric energy furnished to customer at and past the point of delivery,'" a utility "did not have a duty to check equipment downstream to insure it was installed and maintained properly"); Braun v. New Hope Twp., 646 N.W.2d 737, 743 (S.D. 2002) (holding that the responsibility to prevent a motorist's injuries shifted from farmers who broke a warning sign to a township that had a statutory duty to erect guards and maintain warning signs). In other cases, the determination is a result of a number of factors, such as "the degree of danger and the magnitude of the risk of harm, the character and position of the third person . . . his knowledge of the danger and the likelihood that he will or will not exercise proper care, his relation to the plaintiff or to the defendant, and the lapse of time." RESTATEMENT (SECOND) OF TORTS § 452 cmt. f (1965). In some cases, the courts seem to implicitly ask whether the defendant did everything reasonable to prevent the harm from occurring. *See, e.g.*, Balido v. Improved Mach., Inc., 105 Cal. Rptr. 890, 902–04 (App. Ct. 1973) (refusing to hold that the responsibility to prevent a

In these cases, the responsibility for preventing the harm has shifted from the original tortfeasor to someone else. While the law typically shies away from the rubric of "shifting responsibility," there are many instances where tort law has embraced the idea in substance, sometimes dressed in the garb of "duty." The rules in some states, mentioned earlier, that say that a possessor of land need do nothing more than warn a licensee of known dangers,[350] or that a mental health professional treating a dangerous patient need only warn the victim or the police,[351] are rules that, in effect, shift the burden of preventing harm from one party to another once a warning is given.

The bargain of capping a cybersecurity plaintiff's damages at the cost of monitoring security if the database possessor provides notification of a security breach is not a bad one. From the standpoint of the data subject, the plaintiff may be better off with a warning and reimbursement for the out-of-pocket costs of vigilance than gambling on a tort action against the database possessor. A tort suit would be fraught with many obstacles: a possibly short statute of limitations[352] if the intruder does not quickly exploit the improperly accessed data; a risk that the court will not find the database possessor's negligence to be a proximate cause of resulting criminal conduct;[353] a likelihood that the economic-loss or "exposure" rules may bar key portions of the damages;[354] and a possibility that the court might find that the database possessor had no duty at all.[355]

Nor is the bargain bad for database possessors. Capping damages at the cost of security monitoring would avoid the risk of catastrophic liability for personal injuries that sometimes occur, the possibility of exposure to property-damage claims, and the chance that a court might narrowly construe the applicability of the economic-loss rule. Some companies faced with the risk of liability from loss of personal data have voluntarily provided affected persons with security-monitoring protection.[356]

---

defective machine from causing harm shifted from the manufacturer, who offered to repair the machine for $500, to the subsequent owner who refused the offer); *see also* Kent v. Commonwealth, 771 N.E.2d 770, 778 (Mass. 2002) (holding that a board's decision to parole a violent inmate pursuant to an INS deportation warrant shifted the duty to prevent harm from the parole board to the INS).

350. *See supra* note 237.

351. *See supra* note 238.

352. The federal government says that victims of data intrusion should "remain vigilant over the next twelve to twenty-four months." Interagency Guidance, *supra* note 239, at 15,753. In some states, the applicable statute of limitations for negligence might be two years, depending on the nature of the claim. *See, e.g.*, TEX. CIV. PRAC. & REM. CODE ANN. § 16.003(a)–(b) (Supp. 2005) (stating that a two-year limitation applies to certain claims for personal injury, property damage, and wrongful death).

353. *See generally* RESTATEMENT (SECOND) OF TORTS § 448 (1965) (discussing whether intentionally tortious or criminal conduct breaks the chain of causation).

354. *See supra* Parts IV.A and B.

355. *See supra* Part II.

356. *See* Eric Dash, *From Data Holders, Lots of Reassurance*, N.Y. TIMES, July 18, 2005, at C6 (discussing a television advertisment highlighting "Citigroup's free identity theft protection services, which include fraud detection warnings on every bank and credit card account"); McCoy, *supra* note 45, at 490–91 (stating that, upon learning of the theft of laptops containing customer information in November 2003, Wells Fargo notified the affected customers and "promised to monitor the at-risk accounts, change the affected account numbers, add a Credit Alert report to customers' credit reports,

Moreover, society would be better off if the law capped damages at the cost of security monitoring in exchange for victim notification whenever there is a security breach. The only ways to minimize the losses stemming from database intrusions (aside from criminal penalties, which seem ineffective) are to spur investment in data security, to discover when intrusions occur, and to warn persons whose interests are at risk. A cap on damages in exchange for notification of security breaches would not undercut the database possessors' incentives to invest in data security. Database possessors would still be subject to state and federal laws that impose various sanctions relating to cybersecurity; they would still face the threats of bad publicity and consumer disaffection resulting from disclosure of security breaches; and at least some possessors (e.g., credit card companies) would still stand to lose millions of dollars as a result of fraudulent use of personal information. However, capping damages at security-monitoring costs would help to ensure that database possessors are not subject to ruinous tort judgments. The cap would create incentives to discover security breaches and to internalize the resulting security-monitoring costs that those intrusions entail. Consumers would also be better able to protect their own interest in the variety of ways discussed above. In addition, the cap on damages might also reduce the threat of overburdening already overworked federal and state courts. The cap would greatly simplify damages issues in cybersecurity cases and guidance from the courts would quickly define the average costs of security monitoring, thereby promoting the settlement of cases. Indeed, limiting liability to security-monitoring damages is also likely to promote insurance coverage of intruder-related losses by making the extent of liability more certain, thereby facilitating the pricing of insurance coverage.[357]

A damages cap should not apply to cases involving egregious conduct. A plaintiff who can establish that the defendant acted with reckless indifference or intentional disregard in failing to protect data should be able to avoid the limitation on liability. Similarly, if the defendant did not disclose a security breach, liability for a breach of the notification duty or of the duty to protect data should extend as far as the usual rules of tort law allow.

A cap on database possessor liability at the costs of security-monitoring damages can be legislatively enacted.[358] However, in the absence of legislation to the contrary, questions relating to duty, proximate causation (including shifting responsibility), and damages have traditionally been in the province of the courts. Quite possibly, state law may permit the courts to determine that if a database

---

provide 24-hour access to specially trained account representatives, and provide a one-year membership to a credit-monitoring reporting service so customers could quickly learn if any of their information was being misused"); *cf.* Reddick, *supra* note 15, at 4 (noting that nine states require businesses to notify consumer-reporting agencies of security breaches).

357. *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 16, at 65–66 (describing available coverage and noting that "[t]he paucity of data on cyberrelated losses makes it difficult to accurately price cyberinsurance policies").

358. *See* Victor E. Schwartz et al., *Medical Monitoring—Should Tort Law Say Yes?*, 34 WAKE FOREST L. REV. 1057, 1059 (1999) ("[T]he inherent complexities and significant public policy concerns surrounding medical monitoring awards, which were noted by the United States Supreme Court in *Metro-North*, suggest that the issue ought to be decided by legislatures, not by courts." (citing Metro-North Commuter R.R. Co. v. Buckley, 521 U.S. 424, 441–44 (1997))).

possessor negligently fails to protect computerized personal information, the database possessor has no legal obligation other than to pay for security-monitoring damages if the database possessor revealed the breach to the data subject.

V. CONCLUSION: SECURITY IN INSECURE TIMES

Modern society is built on fragile foundations of computerized personal data. If this society is to endure and prosper, then it must vigilantly safeguard those foundations. Tort law offers an appropriate legal regime for allocating the risks and spreading the costs of database intrusion-related losses. Tort law can also create incentives, on the part of both database possessors and data subjects, to minimize the harm associated with breaches of database security. Courts and legislatures must consider carefully the role of tort liability in protecting computerized data. If those who make and interpret the laws too hastily conclude that database possessors are not liable for losses occasioned by unauthorized data access—whether because there is no duty, no proximate causation, or no recoverable damages—important opportunities to reduce and distribute the costs of computerized technology will be lost. If liability is too readily assessed, important institutions will be adversely affected, and with them the prosperity of modern society. Security in insecure times requires a sensitive balancing of competing interests. Established tort principles carefully applied to the contemporary problems of cybersecurity and identity theft can perform a key role in protecting the economic foundations of modern life.

*